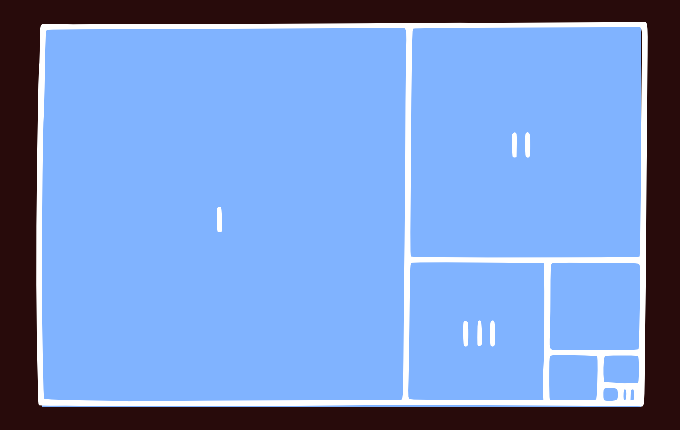
N. Vorobiev

CARACTÈRES DE DIVISIBILITÉ



SUITE DE FIBONACCI

Éditions Mir Moscou

Н. ВОРОБЬЕВ

●

Признаки делимости

Числа Фибоначчи

Издательство «Наука» Москва

N. Vorobiev

CARACTÈRES DE DIVISIBILITÉ

SUITE DE FIBONACCI

Editions Mir · Moscou

CDU 511.92=40

Traduit du russe

На французском языке

$B\frac{0223-272}{041(01)-73}$

Caractères de divisibilité

AVANT-PROPOS

Le cours scolaire de mathématiques actuellement enseigné en U.R.S.S. vise surtout à développer la pensée fonctionnelle, à apprendre aux élèves à manier les objets mathématiques continus. Telle est également l'orientation des modifications qu'on envisage d'apporter aux programmes scolaires de mathématiques en vigueur en Union Soviétique. Par ailleurs, on procède depuis quelque temps à une étude approfondie de nouveaux domaines d'application des mathématiques: composition de programmes pour ordinateurs, certains aspects de la cybernétique et de la recherche opérationnelle, économétrie, linguistique mathématique, etc. L'assimilation de ces branches scientifiques exige, parallèlement à un perfectionnement de l'appareil classique, le développement d'une technique combinatoire et de l'analyse discrète ainsi que la création de fécondes abstractions nouvelles. Toutes ces disciplines méritent certainement qu'on leur réserve aussi une place importante dans les ouvrages de vulgarisation scientifique.



De nombreux sentiers conduisent de la lisière au cœur de la forêt. Ils serpentent, se rejoignent, se séparent de nouveau pour se croiser un peu plus loin. Quand on se promène, on ne peut que remarquer leur abondance, en suivre quelques-uns. Si l'on veut sérieusement étudier la forêt, il faut en parcourir les sentiers jusqu'au bout, tant qu'ils se voient encore parmi les débris végétaux et les broussailles. Pour pouvoir exploiter les produits de la forêt, on est obligé de quitter les sentiers battus et de se frayer un chemin parmi les denses fourrés de buissons épineux.

La présente brochure peut être assimilée à la description d'une promenade à la lisière des mathématiques modernes. L'exposé des faits essentiels se rapportant aux caractères de divisibilité nous fournit un prétexte pour aborder certains

problèmes assez abstraits de mathématiques discrètes. Au nombre de ces problèmes figurent, en premier lieu, les propositions de la théorie élémentaire des nombres groupées autour du théorème fondamental de l'arithmétique et de l'analyse de la décomposition canonique d'un nombre naturel en facteurs premiers. La divisibilité même des nombres est considérée en tant que relation sur un ensemble de nombres entiers, c'est-à-dire en tant que réalisation d'une notion assez générale et abstraite. Enfin nous traitons les caractères de divisibilité comme des algorithmes qui permettent de vérifier si un nombre est divisible par un autre nombre donné. Parmi les caractères de divisibilité, l'auteur a cru bon de mettre surtout l'accent sur les cas des restes égaux.

Pour mettre en relief les diverses relations entre faits mathématiques isolés et la possibilité d'approches différentes, certaines propositions sont démontrées deux fois.

* *
*

Ce livre est destiné aux élèves des classes terminales qui s'intéressent aux mathématiques. A l'exception de quelques références à la formule du binôme, il n'exige aucunes connaissances préliminaires autres que l'aptitude à effectuer d'élémentaires transformations identiques. Toutefois, la structure logique de la matière traitée est assez compliquée, de sorte que l'entière assimilation de celle-ci peut exiger beaucoup d'attention et de patience.

Le lecteur aura intérêt à procéder comme suit.

A la première lecture, on peut se borner au texte principal des §§ 1-3, sans résoudre les problèmes (sauf les problèmes 31, 33, 35, 41, 43, 45 et 46). On se fera ainsi une idée générale des questions abordées. Comme la plupart des profanes en la matière sont convaincus de la justesse du théorème de la décomposition univoque d'un nombre naturel en facteurs premiers (le considérant apparemment comme une sorte d'axiome), ils peuvent comprendre les théorèmes 9-13 comme ses corollaires.

A la deuxième lecture, on doit essayer de démontrer soi-même tous les théorèmes dans l'ordre où ils se présentent.

Pour éviter que le lecteur ne soit trop souvent tenté de se servir des démonstrations toutes prêtes, celles-ci ont été groupées dans une section à part, à l'exception de la démonstration du théorème 7, qui est appelée à donner le ton, en quelque sorte.

A la deuxième lecture, il convient d'étudier le § 4 et de résoudre les problèmes du texte principal.

Finalement, à la troisième lecture, on abordera le texte en petits caractères et les problèmes qui s'y rapportent.

§ 1 DIVISIBILITÉ DES NOMBRES

1. La somme, la différence et le produit de deux nombres entiers sont toujours des nombres entiers. On exprime parfois ce fait en disant qu'un ensemble de nombres entiers *est fermé* par rapport à l'addition, la soutraction et la multiplication.

Par contre, l'ensemble de tous les nombres entiers n'est pas fermé par rapport à la division : d'une façon générale, le quotient de la division d'un nombre entier par un autre nombre entier n'est pas nécessairement entier.

Aussi, quand on étudie les circonstances liées à la division de nombres entiers, l'une des premières questions qui se posent est-elle celle de la possibilité d'effectuer cette opération pour deux nombres donnés, c'est-à-dire de la *divisibilité* de ces nombres. En ce qui concerne les autres opérations arithmétiques sur des nombres entiers, une telle question ne se pose évidemment pas.

Dans la suite nous supposons connues les principales propriétés des opérations arithmétiques sur des nombres entiers ainsi que les propriétés les plus simples des égalités et des inégalités. Sauf mention spéciale, le terme « nombre » désigne toujours un nombre *entier*.

Comme d'habitude, les nombres entiers non négatifs (0, 1, 2, ...) seront appelés *nombres naturels*. S'il s'agit de tous les nombres naturels, nous dirons l'*ensemble de tous les nombres naturels*.

● DÉFINITION. Le nombre a est *divisible* par le nombre b (ou, ce qui revient au même, b est un diviseur de a) s'il existe un nombre c tel que $a = bc$.

Ce fait est appelé *divisibilité* du nombre a par le nombre b et se note $a \vdots b$.

Soulignons que $a \vdots b$ traduit non pas quelque opération à effectuer sur a et b, mais une certaine proposition qui peut

être juste ou fausse selon les valeurs de *a* et *b*. Ainsi, 4 : 2 est juste, tandis que 4 : 3 ne l'est pas.

On dispose d'un assez grand nombre de procédés pour vérifier si la proposition a : b est juste ou non, c'est-à-dire si *a* est divisible par *b*. L'un de ces procédés consiste à effectuer la division de *a* par *b*. Cependant, cette operation s'avère souvent trop longue et laborieuse et l'on éprouve naturellement le désir d'établir la divisibilité sans effectuer la division même. Par ailleurs, et c'est là une considération qui n'est nullement superflue, il se peut fort bien qu'on s'intéresse *uniquement* au fait de savoir si le nombre *a* est divisible par le nombre *b*. En effectuant une division, on trouve aussi en passant le quotient de cette division ainsi que son reste (si la division n'est pas exacte) ; or, en l'occurrence, tous ces nombres n'ont pour nous aucune utilité, puisque la seule chose qui importe est de savoir si le reste de la division est oui ou non égal à zéro. On a donc des raisons de supposer qu'en effectuant la division, nous avons dépensé une partie (et non des moindres) de nos efforts en pure perte. On peut espérer que des procédés plus directs qu'une division pure et simple s'avéreront plus rationnels et permettront de parvenir au résultat voulu par une voie plus courte. De tels procédés existent. Il s'agit de ce qu'on appelle les *caractères de divisibilité*.

Certains caractères de divisibilité sont certainement déjà connus du lecteur. Le but du présent ouvrage est d'examiner divers caractères de divisibilité surtout d'un point de vue de principe.

L'idée de tout caractère de divisibilité par un nombre donné *b* est de ramener la question de la divisibilité d'un nombre *a* par *b* à celle de la divisibilité par *b* d'un certain nombre inférieur à *a* (on conçoit aisément que c'est également l'idée du procédé utilisant une division ordinaire).

De la sorte, un caractère de divisibilité se trouve être un objet mathématique d'une nature très répandue, encore qu'elle ne saute pas aux yeux. Il ne s'agit pas d'une formule,

d'un théorème ou d'une définition, mais d'un certain *processus* exactement du même genre que l'opération qui consiste à multiplier deux nombres par la méthode usuelle, ou encore le calcul l'un après l'autre des termes d'une progression arithmétique.

La notion de caractère de divisibilité sera précisée au paragraphe suivant.

2. La définition de la divisibilité des nombres ne nous renseigne pas sur le nombre de valeurs différentes que peut prendre le quotient de la division de a par b. Tirons cette question au clair une fois pour toutes.

Soit

$$a = bc \tag{1}$$

et par ailleurs

$$a = bc_1.$$

On en déduit que

$$bc = bc_1$$

ou

$$b(c - c_1) = 0.$$

Si, d'autre part, $b \neq 0$, on a $c - c_1 = 0$, c'est-à-dire que $c = c_1$. Si, par contre, $b = 0$, alors $a = 0$, et l'égalité (1) est vraie quel que soit c.

De la sorte, seul 0 est divisible par 0, et le quotient d'une telle division est indéterminé. C'est précisément ce que l'on a en vue quand on parle de l'impossibilité de diviser par 0. Si, au contraire, le diviseur est non nul et que le dividende soit divisible, le quotient a une seule valeur parfaitement définie.

Toutes les fois qu'il sera question de division, nous supposerons le diviseur différent de zéro.

Etablissons quelques-unes des propriétés les plus simples de la divisibilité.

● THÉORÈME 1. $a \,\vdots\, a$.

La divisibilité est *réflexive*.

● THÉORÈME 2. *Si* $a \vdots b$ *et* $b \vdots c$, *alors* $a \vdots c$.

La divisibilité est *transitive*.

● THÉORÈME 3. *Si* $a \vdots b$ et $b \vdots a$, *on a soit* $a = b$, *soit* $a = -b$ (la divisibilité est *antisymétrique*).

● THÉORÈME 4. *Si* $a \vdots b$ *et* $|b| > |a|$, *alors* $a = 0$.

● CONSÉQUENCE. Si $a \vdots b$ et $a \neq 0$, alors $|a| \geqslant |b|$.

● THÉORÈME 5. *Pour que* $a \vdots b$, *il faut et il suffit que* $|a| \vdots |b|$.

Ce théorème nous permet de nous borner au cas où le diviseur est un nombre positif.

● THÉORÈME 6. *Si* $a_1 \vdots b$, $a_2 \vdots b$, . . ., $a_n \vdots b$, *on a*

$$a_1 + a_2 + \ldots + a_n \vdots b.$$

● CONSÉQUENCE. Si la somme de deux nombres et l'un des termes sont divisibles par un nombre b, l'autre terme l'est également.

Tous ces théorèmes ne doivent pas être considérés comme évidents et susceptibles de se passer de démonstrations. Outre qu'en mathématiques toute proposition autre que les axiomes et les définitions doit nécessairement être démontrée, les preuves de ces faits (par exemple de celui que chaque nombre divise lui-même) sont indispensables du point de vue de principe, car ne pouvant être déduites de la seule définition de la divisibilité, elles exigent qu'on ait recours aux propriétés des nombres eux-mêmes.

L'exemple suivant nous aidera à rendre ce point plus explicite.

On sait que la somme, la différence et le produit de nombres pairs sont toujours des nombres pairs. Cependant, la division d'un nombre pair par un nombre pair n'est pas toujours possible et quand elle l'est, le quotient n'est pas forcément un nombre pair. Aussi peut-on introduire la notion de divisibilité paire de nombres pairs.

● DÉFINITION. La *divisibilité* d'un nombre pair a par un nombre pair b *est paire* s'il existe un nombre pair c tel que $a = bc$.

Il est évident que le théorème 1 n est pas vrai pour le cas de la divisibilité paire, car il n'existe pas, par exemple, de nombre pair c tel que $a = ac$.

Nous aurons encore plusieurs fois l'occasion de revenir sur les questions de divisibilité paire de nombres pairs. L'exemple de la divisibilité paire montre qu'on peut concevoir diverses théories de la divisibilité à propriétés différentes et que des théorèmes qui sont justes pour certaines de ces théories peuvent s'avérer faux pour d'autres.

Problèmes. Démontrer que

1. $0 \vdots a$.

2. $a \vdots 1$.

3. Si $1 \vdots a$, alors $a = 1$.

4. Quel que soit $a \neq 0$, il existe un b différent de a tel que $b \vdots a$.

5. Pour tout a, il existe un b tel que $b \vdots c$ et $c \vdots a$ entraînent soit $c = b$, soit $c = a$.

6. Démontrer pour la divisibilité paire les théorèmes analogues aux théorèmes 2, 3, 4 et 5.

7. Elaborer une théorie de la divisibilité telle que les théorèmes 1, 3 et 4 soient justes mais non les théorèmes 2 et 6.

3. Quand on se familiarise même très superficiellement avec les faits concrets de la divisibilité, on est immédiatement frappé par la circonstance suivante: la divisibilité des nombres est pratiquement indépendante de leur grandeur. Ainsi, alors qu'il y a de petits nombres à un nombre relativement élevé de diviseurs (6 pour le nombre 12, à savoir, 1, 2, 3, 4, 6 et 12 et 12 pour 60), certains grands nombres n'en ont que deux (conformément au théorème 1 et au problème 2, chaque nombre différent de l'unité est divisible par deux nombres distincts au moins). On connaît des lois qui régissent la relation qui existe entre la divisibilité d'un nombre et sa grandeur, mais elles sont si compliquées que nous les laisserons de côté.

4. On note avec un intérêt d'autant plus grand que la divisibilité même permet de disposer les nombres selon un cer-

tain ordre qui, tout en différant de leur ordre naturel, n'en présente pas moins avec celui-ci bien des points en commun.

En effet, réfléchissons à ce que signifie exactement la possibilité de disposer des nombres dans l'ordre naturel. Cette possibilité, on le voit aisément, implique que deux nombres naturels quelconques a et b vérifient la relation :

$$a \geqslant b,$$

c'est-à-dire que la différence $a - b$ est non négative (autrement dit qu'il doit exister un nombre naturel c tel que $a = b + c$). Or, le phénomène de divisibilité signifie que deux nombres quelconques a et b vérifient une condition parfaitement définie (à savoir il existe un nombre entier c tel que $a = bc$) ! De la sorte, la relation de divisibilité et la relation $\geqslant$ sont de même nature, ce qui fait qu'on peut parler de leurs propriétés communes ou, au contraire, les opposer l'une à l'autre.

En particulier, à l'instar de la relation de divisibilité, la relation $\geqslant$ entre deux nombres naturels constitue une certaine proposition qui peut être juste (par exemple, $5 \geqslant 3$) ou fausse (par exemple, $3 \geqslant 5$).

Notons immédiatement que la relation $\geqslant$ présente plus de propriétés communes avec la relation de divisibilité que la relation $>$. Cela s'explique par le fait que, de même que la relation de divisibilité, la relation $\geqslant$ est réflexive (en effet, $a \geqslant a$ est juste pour n'importe quel a), tandis que la relation $>$ ne l'est pas (l'inégalité $a > a$ n'est jamais vraie). Aussi considère-t-on en l'occurrence en qualité de relation d'ordre entre nombres naturels la relation $\geqslant$ et non la relation $>$, qui pourrait sembler à première vue plus simple et plus naturelle.

5. La relation $\geqslant$ possède les propriétés suivantes qu'on vérifie aisément :

1° $a \geqslant a$ (réflexivité).
2° Si $a \geqslant b$ et $b \geqslant a$, alors $a = b$ (antisymétrie).
3° Si $a \geqslant b$ et $b \geqslant c$, alors $a \geqslant c$ (transitivité).

4° Toute suite naturelle

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant \ldots \geqslant a_n \geqslant \ldots,$$

dont tous les termes sont distincts, a un dernier terme. On dit alors que la relation d'ordre est une relation d'ordre *total* dans un ensemble de nombres naturels.

Cette dernière propriété est assez compliquée à formuler et présente un caractère quelque peu artificiel. Cependant, elle révèle des traits extrêmement importants de la structure d'un ensemble de nombres naturels muni d'une relation d'ordre notée $\geqslant$. On en déduit de nombreuses autres propriétés de cette relation. De plus, nous verrons que c'est précisément sur cette propriété que se fondent les raisonnements par récurrence auxquels on a si souvent recours dans diverses questions de mathématiques.

En qualité d'application utile de cette propriété, notons la suivante : il existe un nombre a tel que $a \geqslant b$ entraîne $a = b$ (a et b sont des nombres naturels).

En effet, si un tel nombre n'existait pas, nous pourrions d'après chaque a_n trouver un nombre a_{n+1} tel que $a_n \geqslant a_{n+1}$ et $a_n \neq a_{n+1}$. En commençant par un nombre a_1 quelconque, nous obtiendrions la suite

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant \ldots \geqslant a_n \geqslant a_{n+1} \geqslant \ldots$$

qui ne se termine jamais. Or, l'existence d'une telle suite est contraire à l'existence de la relation *d'ordre total* dans un ensemble de nombres naturels.

De la sorte, le nombre a existe effectivement. On l'appelle *premier* nombre ou nombre *minimal* (c'est évidemment 0). Notons que nous n'avons pas, en l'occurrence, établi l'unicité du nombre minimal. Cette unicité sera prouvée plus loin par une voie indirecte.

5° Quel que soit a, il existe un nombre b distinct de a tel que $b \geqslant a$.

On dit alors que l'ensemble de nombres naturels est *illimité* au sens de la relation $\geqslant$.

6° Pour tout $a \neq 0$, il existe un b tel que $a \geqslant b$, $a \neq b$, et pour tout c, $a \geqslant c \geqslant b$ implique soit $c = a$, soit $c = b$. Intuitivement, tout nombre naturel sauf 0 possède un antécédent et un seul (autrement dit, l'ensemble de tous les nombres inférieurs à un nombre donné possède un élément maximal).

7° $a \geqslant b$ ou $b \geqslant a$ (*dichotomie*). En mathématiques, le terme de dichotomie (du grec *dikhotomia*, division en deux parties égales) exprime généralement la réalisation obligatoire de l'une de deux possibilités.

Soulignons que 1°-7° sont les propriétés de la *relation même* sur l'ensemble de tous les nombres naturels et non les propriétés de

tels ou tels nombres liés par cette relation. Aussi certaines d'entre elles peuvent-elles s'avérer fausses pour une relation entre deux nombres basée sur un autre critère quelconque.

Problème 8. S'appuyant uniquement sur les propriétés 1°-7° de la relation $\geqslant$ et sans se servir de propriétés quelconques des nombres mêmes et des opérations sur ces nombres

a) démontrer l'unicité du nombre minimal,

b) démontrer l'unicité de l'antécédent,

c) formuler la définition du successeur d'un nombre donné a (c'est-à-dire du nombre $a+1$) ; prouver son existence et son unicité.

Problème 9. Vérifier lesquelles des propriétés 1°-7° restent vraies pour la relation $>$.

6. La validité des propriétés de la relation $\geqslant$ (de même que de toute autre) peut être établie de deux façons. Premièrement, on peut se servir des propriétés de tels ou tels nombres ou des particularités de structure connues de l'ensemble de tous les nombres naturels. C'est précisément ainsi que nous avons vérifié les propriétés 1°-7°. Deuxièmement, on peut, après s'être assuré de la validité des propriétés 1°-7°, faire abstraction du fait que la relation $\geqslant$ est une relation binaire et établir les autres propriétés de cette relation uniquement à partir de 1°-7°. C'est ainsi que nous avons prouvé l'existence d'un nombre minimal et les propositions du problème 8.

La deuxième approche dite *axiomatique* est très courante en mathématiques modernes : on établit certains *axiomes* (en l'occurrence, ce sont les propositions 1°-7°) qui reflètent les propriétés essentielles des objets étudiés et se passent de démonstrations ; puis, à partir de ces propriétés, on déduit par voie purement logique (sans recourir de nouveau aux propriétés des objets étudiés) toutes les autres propositions qu'on qualifie de *théorèmes.*

Il semblera peut-être à certains de nos lecteurs que l'examen des propriétés des relations indépendamment des objets pour lesquels elles sont définies (des nombres, par exemple) constitue le summum de l'abstraction mathématique dont on n'a absolument que faire dans la vie pratique. A ce propos, deux remarques s'imposent.

Premièrement, outre que, du point de vue des mathématiques modernes, tous les raisonnements que nous tenons ici ne sont nullement abstraits, de nos jours les mathématiciens sont appelés à étudier simultanément de nombreuses relations, voire à établir de nouvelles relations (des relations du «second ordre» en quelque sorte) pour des couples de relations existantes.

L'exposé ci-dessus permet d'illustrer la notion de relation entre relations à l'aide d'un exemple.

Soit une certaine collection de relations α, β, ... entre nombres naturels. Cela signifie que, pour deux nombres quelconques a, b et

pour toute relation γ de la colection, on sait si le couple a, b vérifie la relation γ. Si la relation γ porte sur a et b, on écrit $a\gamma b$.

On dit que la relation α est *plus forte* que la relation β et on note $\alpha \supset \beta$ si deux nombres quelconques vérifiant la relation β vérifient également la relation α, c'est-à-dire si $a\beta b$ entraîne $a\alpha b$.

Ainsi, en désignant la relation de divisibilité paire par $\underset{\text{pair}}{\vdots}$, on peut écrire $\vdots \supset \underset{\text{pair}}{\vdots}$ Ensuite, il est évident que $\geqslant \supset >$. Au contraire, on n'a ni $\vdots \supset \geqslant$ ni $\geqslant \supset \vdots$, car la relation de divisibilité et la relation $\geqslant$ ne sont pas liées par la relation $\supset$. C'est ce que nous avons expliqué au numéro 3.

Certes, pour manipuler à son aise des notions aussi complexes que les relations entre relations, un entraînement spécial est indispensable.

Deuxièmement, des raisonnements de ce genre, voire encore plus abstraits, se rencontrent de plus en plus souvent dans les applications des mathématiques à l'économie, la biologie, la linguistique et l'art militaire. Malheureusement, des explications plus détaillées à ce sujet nous entraîneraient trop loin.

7. Le fait pour un ensemble de nombres naturels d'être ordonné par la relation $\geqslant$ est étroitement lié à la possibilité d'utiliser la méthode de l'*induction complète* ou le *raisonnement par récurrence*. Ci-dessous le schéma de ce mode de raisonnement.

Soit une propriété $A(n)$ d'un nombre naturel n. En fait, cela signifie que nous avons affaire à une suite infinie de propriétés

$$A(0),\ A(1),\ \ldots,\ A(n), \ldots$$

de chacun des nombres naturels. Supposons que

a) $A(0)$ *) est vraie;

b) pour tout n $A(n)$ entraîne $A(n+1)$.

Avec les hypothèses a) et b) $A(n)$ est vraie pour tout nombre naturel n.

---

*) Le raisonnement par récurrence peut être aussi fait à partir de 1.

Le raisonnement par récurrence ne constitue pas une proposition indépendante, il peut être déduit des propriétés 1°-7° relatives à l'ordre d'un ensemble de nombres naturels muni de la relation $\geqslant$.

En effet, supposons que les hypotèses a) et b) soient vérifiées pour la propriété $A(n)$, mais que la conclusion ne soit pas valable. Cette dernière circonstance signifie qu'il doit exister des nombres m tels que $A(m)$ soit fausse. Soit m_1 l'un de ces nombres. Si $A(n)$ est vraie pour tous les $n < m_1$, m_1 est le plus petit des nombres pour lesquels $A(n)$ n'est pas juste. Si, par contre, $A(n)$ n'est juste que pour certains $n < m_1$, il doit exister un $m_2 < m_1$ tel que $A(m_2)$ soit faux.

En définitive, nous obtenons une suite de nombres distincts

$$m_1 > m_2 \geqslant \ldots \geqslant m_r \geqslant \ldots, \tag{2}$$

pour chacun desquels $A(m)$ n'a pas lieu. D'après la propriété 4° de la relation $\geqslant$, le dernier terme de la suite (2) doit être m_r. Il est évident que le nombre m_r est le plus petit de tous les nombres pour lesquels $A(n)$ est faux.

Etant donné que $A(0)$ est juste par hypothèse, $m_r \neq 0$, de sorte qu'il existe un nombre m_r^*, l'antécédent de m_r (en fait ce nombre est $m_r - 1$). Etant donné que $m_r^* < m_r$, la proposition $A(m_r^*)$ doit être vraie. Mais alors, d'après l'hypothèse b) du raisonnement par récurrence, $A(m_r^* + 1)$, c'est-à-dire $A(m_r)$, doit être vraie elle aussi, et nous aboutissons à une contradiction. Donc, il n'y a pas de nombres m pour lesquels $A(m)$ ne soit pas valable.

Une remarque s'impose. Les raisonnements ci-dessus ne sont pas une démonstration ni une justification de la méthode. Ils signifient seulement qu'il est possible de déduire une proposition mathématique d'autres propositions (des propriétés de la relation $\geqslant$). Quant à ces propriétés, nous les avons admises en qualité d'axiomes et nous ne faisions que les vérifier. Toute tentative de les démontrer impliquerait inévitablement la nécessité d'introduire de nouvelles conditions sous forme d'axiomes.

En particulier, la démonstration des propriétés relatives à l'ordre total exige toujours un raisonnement par récurrence (le lecteur s'en assurera lui-même).

Dans la suite nous aurons souvent recours à ce mode de raisonnement.

Problème 10. Supposons que des couples d'objets de nature quelconque (nombres, points, fonctions, théorèmes, etc.) sont liés par une relation $\succeq$ aux propriétés analogues aux 1°-7°. Démontrer que ces objets (éléments) peuvent alors être numérotés (c'est-à-dire inscrits dans un certain ordre): $A_1, A_2, A_3, \ldots$ de telle sorte que $A_i \succeq A_j$ si et seulement si $i \geqslant j$.

Fig. 1

Ce que nous venons de dire signifie, au fond, que la relation munie des propriétés 1°-7° ordonne l'ensemble en une chaîne linéaire d'éléments :

$$A_1 \ni A_2 \ni A_3 \ni \dots$$

8. Revenons à la relation de divisibilité. En cas de nombres positifs, les théorèmes 1, 2, 3 et les problèmes 3, 4 et 5 montrent que, dans les propositions 1°-6°, la relation $\geqslant$ peut être remplacée par la relation $\vdots$. Quant à la proposition 7°, appliquée à la divisibilité, elle s'énonce ainsi : « de deux nombres, un au moins est divisible par l'autre ». Or, cela est faux. De la sorte, la relation de divisibilité possède toutes les propriétés de la relation d'ordre à l'exception d'une seule. En conséquence, la relation de divisibilité ordonne des nombres naturels non sous la forme d'une chaîne linéaire, mais d'une manière différente, plus complexe (voir fig. 1). Remarquons que les nombres proches quant à leur grandeur s'avèrent assez « éloignés » l'un de l'autre du point de vue de leur divisibilité, témoin les nombres 4 et 5 ou 7 et 8.

Passons de la divisibilité de nombres entiers positifs à celle des nombres naturels, autrement dit introduisons le zéro. Dans ce cas, le schéma de la figure se complétera d'une case au-dessus de toutes les

autres, car le zéro se divise par n'importe quel nombre, tandis qu'aucun nombre non nul n'est divisible par 0.

Nous laissons au lecteur le soin de formuler et de vérifier les propositions 1°-7° pour ce cas.

9. DÉFINITION. Toute relation $\succeq$ vérifiant les conditions:

1° $a \succeq a$ (réflexivité),

2° $a \succeq b$ et $b \succeq a$ entraînent $a = b$ (antisymétrie),

3° $a \succeq b$ et $b \succeq c$ entraînent $a \succeq c$ (transitivité),

est une *relation d'ordre partiel*. Les relations d'ordre partiel jouent un grand rôle en l'absence d'un « véritable » ordre total, par exemple là où chaque objet est décrit ou évalué d'après plusieurs indices différents et qualitativement incomparables.

On peut prendre pour exemple le classement d'une épreuve sportive combinée. Si l'une des équipes s'est classée première dans toutes les disciplines, il est évident qu'on peut la considérer comme ayant obtenu de meilleurs résultats. Mais si elle a été victorieuse dans toutes les compétitions sauf une, celle de croquet mettons, où elle a été battue par son adversaire, la question du classement général n'est déjà plus si facile à résoudre. Les mordus du croquet peuvent même insister pour que l'équipe ayant remporté la victoire dans cette discipline soit classée avant l'autre. En tout cas, un classement général doit dépendre de certains calculs conventionnels des points obtenus.

10. Les conditions 1°-3° dont l'observation fait de $\succeq$ une relation d'ordre partiel sont peu précises. Aussi les ensembles partiellement ordonnés (qui le sont d'ailleurs de manières très différentes) sont composés d'éléments les plus divers. A cet égard, quand on dit d'une relation quelconque que c'est une relation d'ordre partiel, on ne saurait ajouter grand-chose à cette qualification. Ainsi, on ne saurait, en général, à l'égard d'objets pour lesquels on a défini une relation d'ordre partiel recourir à la méthode de la récurrence mathématique.

Complétons cependant les conditions 1°-3° par les suivantes:

4° ordre total,

5° ensemble illimité,

6° chaque élément différent de l'élément minimal est le suivant d'un autre nombre unique,

8° chaque élément est précédé d'éléments en nombre fini,

9° quels que soient a et $b \succeq a$ $(b \neq a)$, il existe un nombre c prédécesseur de b tel que $c \succeq a$.

Il s'avère que l'existence d'un ensemble de nombres naturels partiellement ordonné par une relation, satisfaisant aux conditions 1°-6°, 8° et 9°, permet une forme un peu modifiée du raisonnement par récurrence.

Soit de nouveau $A(n)$ une propriété d'un nombre n. Supposons que

a) $A(a)$, où a est un nombre minimal au sens de la relation d'ordre $\succ$, est vraie,

b) si n est un nombre quelconque et que $A(m)$ soit vraie pour tous les m tels que $n \succ m$ et $n \neq m$, $A(n)$ est vraie.

Selon ce type de raisonnement si les conditions a) et b) sont vérifiées, $A(n)$ est juste pour n'importe quel n.

Problème 11. Déduire une « nouvelle forme » du raisonnement par récurrence de sa « vieille forme ».

Comme la relation de divisibilité satisfait aux conditions 1°-6°, 8° et 9° (formulez et vérifiez les relations 8° et 9° pour la relation de divisibilité), ce mode de raisonnement peut s'appliquer et s'énonce comme suit : si une propriété $A(n)$ est vraie pour $n = 1$ et si, la supposant vraie pour tous les diviseurs du nombre n différents de n, on peut démontrer sa validité pour n, alors $A(n)$ est vraie pour n'importe quel nombre.

11. Comme on l'a vu, il n'est pas toujours possible d'effectuer la division exacte de nombres entiers. Aussi est-il utile d'examiner parallèlement une opération plus générale, toujours possible et qui, quand la division se fait exactement, coïncide en fait avec celle-ci. Il s'agit de la *division avec reste*.

● DÉFINITION. *Diviser avec reste* un nombre a par un nombre b ($b > 0$), c'est représenter a sous la forme

$$a = bq + r, \quad 0 \leqslant r < b.$$

q est appelé *quotient incomplet* et r *reste* de la division de a par b. Il est évident que $r = 0$ si et seulement si $a \vdots b$. Dans ce cas, q est égal au quotient de la division de a par b.

Démontrons qu'on peut toujours effectuer une division avec reste et que le quotient incomplet et le reste sont bien définis par le dividende et le diviseur, c'est-à-dire uniques.

Soit d'abord $a \geqslant 0$. Formons une suite de nombres

$$a,\ a - b,\ a - 2b,\ \ldots \tag{3}$$

jusqu'à ce qu'on ait un nombre négatif (il est évident qu'il apparaîtra tôt au tard *)). Supposons que le dernier des ter-

---

*) Pour être plus exact, cela résulte de l'ordre total d'un ensemble de nombres naturels muni de la relation $\geqslant$.

mes non négatifs de la suite (3), c'est-à-dire le plus petit d'entre eux, soit le nombre $a - bq$. En le désignant par r, on a

$$a = bq + r. \tag{4}$$

Il est évident que $r < b$ (sinon le nombre $r - b$, c'est-à-dire $a - (q + 1)\, b$, serait non négatif, ce qui est impossible, car r est *le plus petit* des nombres non négatifs de (3)). De la sorte, (4) est la représentation cherchée du nombre a.

Supposons maintenant que $a < 0$. En raisonnant de façon analogue, écrivons une suite de nombres

$$a,\ a + b,\ a + 2b,\ \ldots$$

jusqu'au premier nombre r non négatif (on vérifie aisément que $r < b$). Supposons que

$$r = a + bq',$$

auquel cas, en désignant $-q'$ par q, on a

$$a = bq + r,$$

C.Q.F.D.

Nous avons ainsi prouvé qu'on peut toujours effectuer une division avec reste.

Démontrons maintenant l'unicité de cette division, c'est-à-dire que si

$$a = bq + r \tag{5}$$

et si

$$a = bq_1 + r_1, \tag{6}$$

on a $q = q_1$ et $r = r_1$.

On ne saurait se dispenser d'une telle démonstration de l'unicité en arguant du fait que, comme l'opération de soustraction est univoque, la suite (3) peut être construite de façon unique; son dernier terme non négatif est également bien défini; supposons que ce soit notre r . . ., etc. Un tel

raisonnement n'élimine pas l'éventuelle obtention d'autres valeurs de q et de r par quelque voie absolument différente.

En comparant les relations (5) et (6), on voit que

$$bq + r = bq_1 + r_1,$$

d'où

$$r - r_1 = b(q_1 - q),$$

c'est-à-dire que $r = r_1$ est divisible par b. Mais $|r - r_1| < b$ et, d'après le théorème 4, cela n'est possible que pour $r - r_1 = 0$, c'est-à-dire pour $r = r_1$. Mais alors

$$b(q_1 - q) = 0$$

et, comme le nombre b est différent de zéro, $q_1 - q = 0$, donc $q_1 = q$. L'unicité de la division avec reste est ainsi prouvée.

De la sorte, nous avons démontré le théorème suivant.

● THÉORÈME 7 (relatif à la division avec reste). *Pour des nombres quelconques a et b ($b > 0$), des nombres r et q tels que $a = bq + r$, $0 \leqslant r < b$, existent et sont uniques.*

Problème 12. Formuler et démontrer le théorème sur la division avec reste pour une divisibilité paire.

12. DÉFINITION. Un nombre p différent de l'unité est *premier* s'il n'a pas d'autres diviseurs que lui-même et l'unité.

Comme exemples simples de nombres premiers, citons les nombres 2, 3, 5, 7, 11, 13, etc.

Un nombre différent de l'unité et non premier est dit *composé*.

● THÉORÈME 8. *La suite des nombres premiers est illimitée.*

Tout nombre qui divise à la fois les nombres a et b est appelé *diviseur commun* à ces nombres. Le plus grand des diviseurs communs aux nombres a et b est leur *plus grand commun diviseur* qu'on note PGCD (a, b).

Si le plus grand commun diviseur de a et b est égal à l'unité, ces nombres sont *premiers entre eux*.

En d'autres termes, a et b sont premiers entre eux s'ils n'ont d'autre diviseur commun que l'unité.

● THÉORÈME 9. *Si a et p sont des nombres naturels et que, de plus, p soit premier, alors on a ou bien $a \vdots p$, ou bien a et p sont premiers entre eux.*

Tout nombre divisible à la fois par les nombres a et b est appelé *multiple commun* à ces nombres. Parmi tous les multiples positifs communs à a et b, le plus petit est appelé *le plus petit commun multiple* de ces nombres.

● THÉORÈME 10. *Si M est le multiple commun à a et b et m leur plus petit commun multiple, alors $M \vdots m$.*

● THÉORÈME 11. *Le plus petit commun multiple de deux nombres premiers entre eux est égal à leur produit.*

● CONSÉQUENCE. Pour qu'un nombre a soit divisible par des nombres b et c premiers entre eux, il faut et il suffit qu'il soit divisible par leur produit.

● THÉORÈME 12. *Si $ab \vdots c$ et b et c sont premiers entre eux, alors $a \vdots c$.*

● THÉORÈME 13. *Si le produit de plusieurs facteurs est divisible par un nombre premier p, l'un au moins des facteurs est divisible par p.*

● CONSÉQUENCE. Si p est premier, $0 < k < p$, le nombre

$$C_p^k = \frac{1 \cdot 2 \ldots (p-1)\, p}{1 \cdot 2 \ldots (k-1)\, k \cdot 1 \cdot 2 \ldots (p-k-1)(p-k)}$$

est divisible par p.

● THÉORÈME 14. (théorème fondamental de l'arithmétique). *Tout entier positif différent de l'unité est décomposable d'une seule manière en facteurs premiers* (les produits qui ne diffèrent que par l'ordre de leurs facteurs sont identiques).

Le théorème fondamental de l'arithmétique montre qu'il est en principe possible de décomposer n'importe quel nombre en facteurs premiers. Cependant, en pratique, cette décomposition se heurte parfois à de grandes difficultés que les mathématiques modernes ne sont pas encore toujours en mesure de surmonter. Pour décomposer de grands nombres en facteurs premiers ou vérifier s'ils sont premiers, on se sert actuellement d'ordinateurs. Ainsi, on n'a établi qu'en 1957 que le nombre $2^{3217} - 1$ est premier; comportant 969 chiffres, c'est le plus grand des nombres premiers actuellement connus. Il a fallu 5 heures et demie à un ordinateur rapide pour prouver qu'il s'agit d'un nombre premier.

Soit un certain nombre a décomposé en facteurs premiers. En groupant les facteurs égaux, on obtient la formule suivante:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{7}$$

où $p_1, p_2, \dots, p_r$ sont des nombres premiers distincts et $\alpha_1, \alpha_2 \dots, \alpha_r$ des entiers positifs. Le produit du deuxième membre de la formule (7) est appelé *décomposition canonique* du nombre a.

● THÉORÈME 15. *Pour que des nombres a et b soient premiers entre eux, il faut et il suffit qu'aucun des facteurs premiers faisant partie de la décomposition canonique de a ne figure dans la décomposition canonique de b.*

● THÉORÈME 16. *Soit* (7) *la décomposition canonique du nombre a. Dans ce cas, pour que b soit divisible par a, il faut et il suffit que*

$$b \,\vdots\, p_1^{\alpha_1}, \quad b \,\vdots\, p_2^{\alpha_2}, \dots, b \,\vdots\, p_r^{\alpha_r}.$$

Il découle des théorèmes 15 et 16 que la divisibilité par un produit de plusieurs nombres premiers entre eux équivaut à la divisibilité simultanée par chacun d'entre eux.

Problème 13. Majorer le plus petit diviseur premier du nombre non premier a.

Problème 14. Soit

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

la décomposition canonique du nombre a. Dans ce cas, pour qu'il y ait divisibilité de a par b, il faut et il suffit que la décomposition canonique de b se présente sous la forme suivante

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r},$$

où $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, ..., $0 \leqslant \beta_r \leqslant \alpha_r$.

Problème 15. Désignons par $\tau(a)$ le nombre de diviseurs distincts du nombre a (y compris l'unité et le nombre a lui-même). Démontrer que pour le nombre a dont la décomposition canonique est $p_1^{\alpha_1}, p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, on a :

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Problème 16. Trouver a si $a \vdots 3$, $a \vdots 4$ et $\tau(a) = 14$.

Problème 17. La décomposition canonique du nombre a a la forme $p_1^{\alpha_1} p_2^{\alpha_2}$ et $\tau(a^2) = 81$. Que vaut $\tau(a^3)$?

Problème 18. Calculer a si $a = 2\tau(a)$.

Problème 19. Les analogues des théorèmes 11-14 sont-ils justes pour une divisibilité paire ?

Problème 20. Etant données les décompositions canoniques de deux nombres quelconques, indiquer le procédé de construction des décompositions canoniques du PPCM et du PGCD de ces nombres.

§ 2 DIVISIBILITÉ DES SOMMES ET DES PRODUITS

1. Lors d'une division avec reste, on ne s'intéresse souvent qu'au reste de la division d'un nombre a par un nombre b, la grandeur du quotient incomplet étant inessentielle.

Supposons, par exemple, que l'on veuille savoir quel jour de la semaine sera le 1[er] janvier de l'an 2000 (en supposant, bien entendu, que le calendrier actuellement en vigueur le soit encore à l'époque). On vérifie aisément en consultant le

calendrier correspondant que le 1er janvier 1973 était un lundi. Les 27 ans qui séparent ces dates comprennent $27\times \times 365 + 6$ (ce dernier terme est le nombre des années bissextiles entre 1973 et l'an 2000), soit 9861 jours, soit 1408 semaines et 5 jours. A l'issue de 1408 semaines, ce sera de nouveau lundi ; donc, le 1er janvier de l'an 2000, soit 5 jours plus tard, sera un samedi. Il est évident que pour résoudre le problème ci-dessus, on a besoin de connaître non pas le nombre exact des semaines qui séparent 1973 de 2000, mais seulement le nombre des jours qui s'écouleront au cours de cette période en sus de ces semaines.

Des problèmes de ce genre se posent parfois aux historiens, surtout aux orientalistes, lorsqu'ils comparent les dates indiquées par des calendriers différents.

Il peut sembler que pour trouver le reste de la division d'un nombre par un autre, le plus simple soit d'effectuer directement cette division. Cependant, en pratique, une telle opération s'avère souvent très laborieuse, surtout si, au lieu d'être inscrit dans le système de numération décimale qui nous est familier, le dividende considéré se présente sous la forme de quelque expression compliquée telle que $2^{1000} + + 3^{1000}$, par exemple. Par ailleurs, la plus grande partie de ce travail ira à la détermination du quotient incomplet qui, par lui-même, nous est inutile. Aussi a-t-on intérêt à chercher un procédé qui nous permette de trouver directement le reste sans calculer le quotient incomplet.

Mettons l'un de ces procédés en évidence en l'appliquant à la résolution du problème ci-dessus qui consiste à établir quel jour de la semaine sera le 1er janvier de l'an 2000. On peut tenir le raisonnement suivant. Selon qu'elle est ordinaire ou bissextile, une année comprend 365 jours (soit 52 semaines plus 1 jour) ou 366 jours (soit 52 semaines plus 2 jours). Donc, toute la période qui sépare le 1er janvier 1973 du 1er janvier de l'an 2000 comporte un certain nombre (qui importe peu) de semaines plus un nombre de jours égal à celui des années comprises dans cette période, chaque année

bissextile comptant pour deux. En l'occurrence, ce nombre de jours est de $27 + 6 = 33$. En retranchant 4 semaines de ce nombre, on obtient 5 jours et ce sont eux qu'il convient d'ajouter à notre lundi. On s'aperçoit qu'un tel remplacement d'une année par une journée est la manifestation d'un procédé très général que nous nous proposons d'étudier ci-après.

2. Etablissons quelques propriétés de deux nombres a et b donnant *le même reste* quand on les divise par un même nombre m.

● THÉORÈME 17. *La condition nécessaire et suffisante pour que deux nombres donnés a et b divisés par un nombre m donnent des restes égaux est que leur différence soit divisible par m.*

● THÉORÈME 18. *Lorsque les nombres* $a_1, a_2, \ldots, a_n$ *et* $b_1, b_2, \ldots, b_n$ *donnent des restes égaux si on les divise respectivement par un même diviseur m, il en est de même des nombres* $a_1 + a_2 + \ldots + a_n$ *et* $b_1 + b_2 + \ldots + b_n$*, ainsi que des nombres* $a_1a_2 \ldots a_n$ *et* $b_1b_2 \ldots b_n$.

● CONSÉQUENCE. Si les nombres a et b divisés par m donnent des restes égaux, il en est de même des nombres a^n et b^n pour tout nombre naturel n.

Le théorème 18 et sa conséquence nous fournissent déjà d'assez riches possibilités pour trouver les restes de divisions. En voici quelques exemples.

● EXEMPLE 1. Trouver le reste de la division de

$$A = 13^{16} - 2^{25} \cdot 5^{15}$$

par 3. Il est évident que quand on les divise par 3, le nombre 13 et le nombre 1 donnent le même reste et qu'il en est de même de 2 et -1 et de 5 et -1. Donc, en vertu de ce qui a été démontré, la division de A et de

$$1^{16} - (-1)^{23} (-1)^{15} = 1 - 1 = 0$$

par 3 donne des restes égaux. Le reste cherché est donc 0 et A est divisible par 3.

● EXEMPLE 2. Trouver le reste de la division de ce même nombre A par 37.

Représentons à cet effet le nombre A sous la forme suivante:

$$A = (13^2)^8 - (2^5)^5 \cdot (5^3)^5.$$

Etant donné que $13^2 = 169$ et -16, $2^5 = 32$ et -5, $5^3 = 125$ et $+14$ divisés par 37 donnent respectivement des restes égaux, il en est de même du nombre A tout entier et de

$$(-16)^8 - (-5)^5 (+14)^5,$$

ou, ce qui revient au même, de

$$(16^2)^4 + 70^5.$$

Mais la division de 16^2, c'est-à-dire 256, et de -3 de même que celle de 70 et de -4 par 37 donne des restes égaux. Donc, A et

$$(-3)^4 + (-4)^5,$$

ou, ce qui est la même chose,

$$81 - (2^5)^2$$

et aussi, par conséquent,

$$81 - (-5)^2 = 81 - 25 = 56$$

donnent le même reste quand on les divise par 37.

Finalement, quand on les divise par 37, 56 et 19 donnent le même reste. Etant non négatif et inférieur à 37, 19 est donc le reste cherché.

Problème 21. Trouver les restes des divisions suivantes:

a) $A = (116 + 17^{17})^{21} : 8$,

b) $A = 14^{256} : 17$.

Problème 22. Prouver que pour n'importe quel n:

a) $n^3 + 11n \vdots 6$,

b) $4^n + 15n - 1 \vdots 9$,

c) $10^{3^n} - 1 \vdots 3^{n+2}$,

d) pour un a quelconque

$$a^{2n+1} + (a-1)^{n+2} \vdots a^2 - a + 1.$$

3. Les nombres a et b qui donnent le même reste quand on les divise par m sont dits *congrus modulo* m, ce qui se note

$$a \equiv b \pmod{m}$$

(une telle relation s'appelle *congruence*).

La congruence porte sur des entiers modulo m et jouit des propriétés suivantes:

1° $a \equiv a \pmod{m}$ (réflexivité).

En effet, $a - a = 0 \vdots m$.

2° Si $a \equiv b \pmod{m}$, alors $b \equiv a \pmod{m}$ (symétrie).

En effet, si $a - b \vdots m$, on a : $b - a \vdots m$ (ne serait-ce que d'après le théorème 5).

3° Si $a \equiv b \pmod{m}$ et $b \equiv c \pmod{m}$, alors $a \equiv c \pmod{m}$ (transitivité).

Pour le démontrer, il suffit de noter que, d'après le théorème 6, $a - b \vdots m$ et $b - c \vdots m$ entraînent $a - c \vdots m$.

Si une relation (que nous désignons par $\sim$) est réflexive, symétrique et transitive, elle est appelée *relation d'équivalence*. L'exemple le plus simple d'une relation d'équivalence sur un ensemble de nombres est la relation d'égalité.

Problème 23. Une relation d'équivalence $\sim$ sur un ensemble de nombres partage cet ensemble en classes (appelées classes d'équivalence) telles que deux nombres quelconques d'une même classe soient équivalents et que si deux nombres quelconques ne le sont pas, leurs classes d'équivalence soient disjointes. (Démontrer.)

Dans ce problème, il s'agit d'une relation d'équivalence entre nombres. Mais il est tout aussi valable pour des relations portant sur des objets de nature absolument quelconque.

Etant donné que la congruence modulo m est une relation d'équivalence, elle divise également un ensemble de nombres entiers en classes, appelées *classes résiduelles* modulo m.

4° Le nombre des classes résiduelles modulo m est égal à m.

En effet, les deux nombres a et b appartiennent à la même classe résiduelle modulo m si, et seulement si, ils donnent le même reste quand on les divise par m. Mais ce reste peut prendre exactement m valeurs: $0, 1, 2, \ldots, m-1$. Donc, le nombre de classes est lui aussi égal à m.

Notons à ce propos une circonstance extrêmement intéressante.

Pour que toute classe résiduelle modulo m_1 soit incluse dans une certaine classe résiduelle modulo m_2, il faut et il suffit que $m_1 \vdots m_2$.

En effet, soit K_1 une classe résiduelle modulo m_1 contenant le nombre 0. Il est évident que la classe K_1 contient tous les nombres tels que, divisés par m_1, ils donnent 0 pour reste, c'est-à-dire qui sont divisibles par m_1. En particulier, cette classe contient le nombre m_1. La classe résiduelle modulo m_2 dont fait partie K_1 contient également 0 et, par conséquent, tous les nombres divisibles par m_2. Etant donné que parmi les éléments de cette classe figure le nombre m_1, on doit avoir $m_1 \vdots m_2$. La condition nécessaire est donc démontrée; quant à la condition suffisante, elle est évidente.

De la sorte, la relation de divisibilité peut être déterminée par les relations entre classes résiduelles. Ce procédé permet de déterminer la divisibilité d'objets d'une nature bien plus générale et complexe que les nombres naturels. Le développement conséquent de ces idées conduit à la théorie des groupes, branche majeure de l'algèbre moderne, qui possède des applications importantes en physique théorique et en cristallographie.

Poursuivons l'énumération des propriétés des congruences. Il découle directement du théorème 18 que:

5° Si $a \equiv b \pmod m$ et $c \equiv d \pmod m$, alors

$$a + c \equiv b + d \pmod m.$$

● CONSÉQUENCE. Si $a \equiv b \pmod m$, alors

$$a + r \equiv b + r \pmod m$$

pour tout entier r.

6° Si $a \equiv b \pmod m$ et $c \equiv d \pmod m$, alors

$$ac \equiv bd \pmod m.$$

Les propriétés 5° et 6° montrent qu'à l'instar des égalités les congruences peuvent être additionnées ou multipliées membre à membre.

Problème 24. Si une relation d'équivalence $\sim$ définie sur un ensemble de nombres entiers partage cet ensemble en m classes, $a \sim b$ et $c \sim d$ entraînant $a + c \sim b + d$, cette relation est la congruence modulo m (c'est-à-dire que $a \sim b$ si, et seulement si, $a \equiv b \pmod m$).

Problème 25. Enoncer et démontrer les règles de simplification des congruences.

Problème 26. Si un nombre premier p ne divise pas a, aucuns deux nombres de la suite $a, 2a, 3a, \ldots, (p-1)a$ ne sont congrus modulo p. Aussi en divisant les nombres $a, 2a, 3a, \ldots, (p-1)a$ par p obtient-on tous les restes, sauf 0, chacun une seule fois.

Problème 27. (Théorème de Wilson.) *Pour qu'un nombre p soit premier, il faut et il suffit que* $(p-1)!+1=1\cdot 2\ldots (p-1)+1$ *soit divisible par p.*

Problème 28. Enoncer et démontrer, pour le cas des restes égaux, un théorème analogue au théorème 16.

§ 3 CARACTÈRES DE CONGRUENCE MODULO m ET CARACTÈRES DE DIVISIBILITÉ

1. Voici un procédé très courant pour trouver le reste de la division d'un nombre naturel a quelconque mais fixe par un nombre naturel m donné. Formons la suite de nombres naturels

$$a = A_0,\ A_1,\ A_2,\ \ldots, \tag{8}$$

donnant le même reste quand on les divise par m et cela de sorte que tout terme égal ou supérieur à m soit suivi d'au moins un terme. Il est clair que, dans ce cas, le dernier terme de la suite (8) (s'il existe, évidemment) est égal au reste r de la division de a par m.

L'exemple le plus simple d'une telle suite est la suite (3) du n° 11, § 1. La recherche du reste dans les exemples 1 et 2 du paragraphe précédent se ramène au fond à la construction d'une suite de ce type.

Nous appellerons *caractère de congruence* modulo m tout procédé de construction de la suite (8).

Tel est en particulier le processus de soustractions successives du nombre m jusqu'à ce qu'on obtienne un nombre inférieur à m.

2. Pour être vraiment valable, un caractère de congruence modulo m doit satisfaire aux trois conditions suivantes:

1. Il doit être *exactement défini*, c'est-à-dire que le nombre a doit bien définir tous les termes de la suite (8) sans laisser la moindre place à un arbitraire quelconque.

2. Il doit être applicable à tout entier naturel a. Cette propriété du caractère est ce qu'on appelle son *universalité.*

3. Enfin, l'un au moins des termes de la suite (8) doit être inférieur à m. Autrement dit, la suite (8) doit avoir un nombre fini de termes : la construction de la suite ne peut pas se prolonger indéfiniment, elle se termine tôt ou tard par l'apparition d'un reste de la division de a par m. Cette propriété du caractère de congruence modulo m est son *efficacité*.

Les conditions énumérées peuvent être satisfaites par des moyens très variés, dont le plus naturel est le suivant.

Essayons de trouver une fonction $f(x)$ satisfaisant aux conditions suivantes :

a) pour $x \geqslant m$, $f(x)$ est un nombre naturel,

b) pour $x < m$, $f(x)$ n'est pas définie (autrement dit, n'a pas de sens) (Le fait que telle ou telle fonction perde son sens pour certaines valeurs de la variable n'a rien de surprenant. Ainsi, pour $x = 0$ ou pour $x = 1$, la fonction $\frac{1}{x(x-1)}$ n'a pas de sens.),

c) si $f(x)$ a un sens, $f(x) < x$,

d) si $f(x)$ a un sens, la division de x et $f(x)$ par m donne le même reste.

De telles fonctions existent, telle $f_0(x)$:

$$f_0(x) = \begin{cases} x - m \text{ si } x \geqslant m, \\ \text{n'est pas définie si } x < m. \end{cases}$$

C'est précisément cette fonction qui permet de former la suite (3) du § 1.

A chaque fonction $f(x)$ satisfaisant aux conditions a)-d) correspond un certain procédé de construction de la suite (8), c'est-à-dire un certain caractère de congruence modulo m.

En effet, soit a un nombre naturel quelconque. Formons la suite de nombres

$$A_0,\ A_1,\ A_2,\ \ldots, \tag{9}$$

où $A_0 = a$ et $A_{k+1} = f(A_k)$ pour $k = 0, 1, \ldots$

Si $A_k \geqslant m$, la valeur de la fonction $f(A_k)$ est définie, de sorte que A_k est suivi d'au moins un terme. Si, par contre,

$A_k < m$, $f(A_k)$ n'est pas définie et A_k est le dernier terme de la suite (9).

Ainsi, nous sommes effectivement en présence d'un certain caractère de congruence modulo m.

3. Montrons que ce caractère satisfait aux conditions 1, 2 et 3.

La première condition est remplie parce que chaque terme de la suite (9) définit de façon unique le terme suivant (à condition évidemment que celui-ci existe).

Il y a là une certaine nuance qui, bien qu'elle ne saute pas aux yeux, n'en joue pas moins un rôle extrêmement important. Le fait est que, pour définir la suite (9), avant de calculer une valeur de $f(A_k)$ il nous faut déterminer si cette valeur peut exister d'une façon générale. En d'autres termes, nous devons être en mesure d'établir si le nombre A_k est supérieur ou inférieur à m. Si les nombres A_k et m sont écrits sous une forme commode, par exemple en numération décimale, une telle comparaison se fait aisément. Il en va autrement s'il s'agit de comparer des nombres tels que $2^{20} - 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$ et $3^{10} - 78 \cdot 757$ par exemple, bien que le premier soit égal à 1 et le second à 3.

En conséquence, nous n'appliquons les caractères de congruence qu'aux nombres positifs représentés dans le système de numération décimale.

En ce qui concerne la deuxième condition, il suffit de faire la remarque suivante. Si $a \geqslant m$, on peut en fait commencer à former la suite en calculant la valeur de $f(a)$ qui existe par hypothèse. Si $a < m$, $f(a)$ n'a pas de sens ; cependant, dans ce cas, le nombre a lui-même est le reste de sa division par m, a compose donc toute la suite (9) qui, en l'occurrence, comprend un seul terme.

Passons à la troisième condition. Par hypothèse, la fonction $f(x)$ est choisie de façon que tous les termes de la suite (9) soient de même signe et décroissent en valeur absolue. Comme le premier terme est positif, la suite possède un terme minimal non négatif (le numéro de ce terme, on le vérifie

aisément, ne dépasse pas le nombre a). Si ce terme (désignons-le par α) était supérieur ou au moins égal à m, il existerait une valeur de $f(\alpha)$ toujours non négative et inférieure à α. Donc, le terme α ne serait pas le dernier terme non négatif de la suite (9). Par conséquent, le dernier terme non négatif de (9) doit être inférieur à m. Mais alors, la valeur de $f(\alpha)$ n'a pas de sens et α se trouve être le dernier terme de notre suite. De la sorte, le processus de formation de la suite s'arrête, et le dernier terme de celle-ci est bien le reste de la division de a par m.

Nous avons donc établi que le caractère de congruence décrit est effectivement défini, universel et efficace. Les procédés jouissant de ces trois propriétés sont appelés *algorithmes* et leur rôle dans les mathématiques modernes ne fait que croître. Nous avons déjà donné quelques exemples simples d'algorithmes à la fin du n° 1, § 1. L'exposé ultérieur nous en fournira plusieurs autres.

4. *L'algorithme d'Euclide* est l'un des plus importants en mathématiques.

Soient a et b deux nombres naturels tels que $b < a$. Divisons a par b avec reste: $a = bq_0 + r_1$, $0 \leqslant r_1 < b$. Si $r_1 \neq 0$, nous pouvons diviser b par r_1 avec reste: $b = r_1q_1 + r_2$, $0 \leqslant r_2 < r_1$. Poursuivant ces divisions successives avec reste par le reste de la division précédente nous obtenons les relations suivantes: $r_1 = r_2q_3 + r_3$, $r_2 = r_3q_4 + r_4$, etc.

Montrons que le procédé décrit est effectivement un algorithme, c'est-à-dire qu'il est défini, universel et efficace.

Remarquons qu'il s'agit des divisions successives avec reste. Or, la division avec reste peut toujours se faire et est univoque. On établit également sans grandes difficultés la troisième propriété. Le nombre b et les restes successifs forment évidemment une suite décroissante de nombres non négatifs:

$$b,\ r_1, r_2,\ \ldots \tag{10}$$

Mais le nombre de tous les nombres non négatifs non supérieurs à b est $b + 1$. C'est pourquoi la suite (10) ne peut, elle non plus, comprendre plus de b termes, de sorte que nous pouvons effectuer en

l'occurrence tout au plus b divisions avec reste*). De la sorte, le procédé considéré est effectivement un algorithme.

Explicitons les conditions de la terminaison de l'opération. La dernière division est évidemment telle qu'elle ne peut être suivie d'une autre division par son reste. Or, cela n'est possible que si ce dernier reste est égal à 0, c'est-à-dire si la dernière division se fait exactement.

Problème 29. a) Quand on applique l'algorithme d'Euclide aux nombres a et b, le dernier reste r_n non nul est le PGCD (a, b).

b) Quels que soient les nombres naturels a et b, il existe des nombres entiers A et B tels que $aA + bB =$ PGCD (a, b).

Problème 30. Déduire les théorèmes 9, 12, 13 et 14 du résultat b) du problème 29. (Soulignons que nos raisonnements liés à l'algorithme d'Euclide se fondaient uniquement sur la possibilité d'une division avec reste. Nous n'avons pas eu recours aux théorèmes 9-14 ni à aucune autre considération basée sur le théorème fondamental de l'arithmétique.)

5. Il va sans dire que la description de l'algorithme donnée au nº 3 ne constitue pas sa définition exacte, qui est relativement compliquée et n'a pas sa place ici. Cependant, les exigences mentionnées reflètent assez bien les conditions auxquelles doivent satisfaire les procédés mathématiques appelés algorithmes. On peut définir le rôle des algorithmes en disant qu'il s'agit de procédés uniformes pour résoudre toute une série de problèmes apparentés. Ainsi, les algorithmes dont il vient d'être question permettent de calculer le reste de la division d'un nombre variable a par un nombre fixe m. Les cas particuliers d'algorithmes sont constitués par les calculs de toute sorte qu'on peut effectuer d'après des formules dans lesquelles les lettres peuvent être remplacées par tels ou tels nombres.

On peut dire par un certain abus de langage que tous les problèmes mathématiques dont les solutions peuvent être utomatisées sont des algorithmes. Aussi n'est-ce pas un hasard si le développement de la théorie des algorithmes a coïncidé avec l'apparition et l'emploi généralisé des ordinateurs.

---

*) En réalité, le nombre de ces divisions ne peut dépasser 5 log b. C'est ce qui découle de l'examen de la suite de Fibonacci (cf. la deuxième partie de cette brochure).

On ne ramène pas aux algorithmes les seuls problèmes de calcul au strict sens de ce mot, c'est-à-dire les problèmes dans lesquels on peut, en se servant de règles plus ou moins compliquées et sur la base de données de départ, obtenir une réponse numérique. On peut aussi envisager la recherche d'algorithmes permettant de démontrer n'importe quel problème se rapportant à un certain domaine des mathématiques. De tels algorithmes doivent être capables de transformer les énoncés de théorèmes en leurs démonstrations. Tout surprenant que cela puisse paraître, de tels algorithmes existent, bien que leur application soit limitée à des chapitres des mathématiques assez restreints. Cependant, pour certains domaines (par exemple pour ceux qui contiennent toute l'arithmétique), l'existence de tels algorithmes est en principe impossible.

6. Nous servant du procédé d'élaboration des caractères de congruence modulo m exposé au n° 1, trouvons-en quelques-uns. Dans le cas présent comme par la suite, nous considérerons que les nombres dont il s'agit de trouver les restes de la division par un nombre sont écrits en numération décimale.

Trouvons d'abord le caractère de congruence modulo 5.

Soit A un nombre naturel. Représentons-le sous la forme $10a + b$ (b étant le dernier chiffre du nombre A) et posons

$$f_1(A) = \begin{cases} b \text{ si } A \geqslant 10, \\ b - 5 \text{ si } 5 \leqslant A < 10, \\ \text{n'est pas définie si } A < 5. \end{cases}$$

Nous laissons au lecteur le soin de vérifier que la fonction ainsi définie satisfait aux conditions a)-d) du n° 2.

De la sorte, pour trouver le reste de la division d'un certain nombre par 5, il suffit de prendre le dernier chiffre de ce nombre. Si ce chiffre est inférieur à 5, il s'agit du reste cherché; sinon, on en retranche 5. Notons que l'application de ce caractère à un nombre quelconque conduit à la forma-

tion d'une suite du type (9) comportant au plus trois termes.

Il est évident que tous ces raisonnements visent non pas à découvrir le « caractère de divisibilité » par 5, que tout le monde connaît, mais à le faire par le procédé uniforme décrit au nº 2.

Problème 31. Indiquer et analyser les caractères analogues de congruence modulo 2, 4, 8, 10, 16, 20 et 25.

Problème 32. Représentons le nombre naturel A sous la forme

$$10^k a + b \quad (0 \leqslant b < 10^k)$$

et posons

$$f(A) = \begin{cases} b \text{ si } A \geqslant 10^k, \\ \text{reste de la division de } A \text{ par } m \text{ si } m \leqslant A < 10^k; \\ \text{n'est pas définie si } A < m. \end{cases}$$

Quels sont les modules m pour lesquels un tel algorithme est un caractère de congruence pour un certain k?

7. En qualité de deuxième exemple, considérons le caractère de congruence modulo 3.

Représentons à cet effet le nombre naturel A sous la forme

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10 a_1 + a_0,$$

où $0 \leqslant a_i < 10$ ($a_0, a_1, \ldots, a_{n-1}, a_n$ sont les chiffres du nombre A). Posons

$$f_2(A) = \begin{cases} a_0 + a_1 + \ldots + a_{n-1} + a_n \text{ si } A \geqslant 10, \\ \text{reste de la division de } A \text{ par 3 si } 3 \leqslant A < 10, \\ \text{n'est pas définie si } A < 3. \end{cases}$$

Problème 33. Vérifier que la fonction $f_2(x)$ satisfait aux conditions a)-d) et définit par là même un certain caractère de congruence modulo 3.

Problème 34. Appliquer le caractère de congruence modulo 3 que nous venons d'établir

a) aux nombres 858 773 et 789 988,

b) au nombre qui est représenté en numération décimale par 4444 quatres.

Problème 35. Indiquer et analyser les caractères analogues de congruence modulo 7, 9, 11, 13 et 37.

8. Dans de nombreux problèmes, la valeur du quotient incomplet et aussi celle du reste sont inessentielles et il n'importe de savoir que si ce reste est nul, c'est-à-dire si le premier nombre se divise par le deuxième. Après ce qui a été expliqué au n° 1, nous savons comment aborder les problèmes de ce genre.

Nous dirons que les nombres a et b sont ***équidivisibles*** par m si a et b sont simultanément divisibles ou indivisibles par m.

Problème 36. Quel que soit m, tous les nombres congrus modulo m sont équidivisibles par m. Montrer sur un exemple que la réciproque est fausse.

Problème 37. Quels sont m pour lesquels l'équidivisibilité de deux nombres par m entraîne leur congruence modulo m?

Problème 38. Montrer que la relation d'équidivisibilité par un nombre donné m est une relation équivalente et partage l'ensemble de nombres entiers en deux classes.

Problème 39. Le théorème 18 est-il valable pour des nombres équidivisibles? Et sa conséquence?

9. Soit un nombre A dont il s'agit de trouver s'il est divisible par m. Formons une suite de nombres entiers décroissant en valeur absolue

$$A = A_0, A_1, A_2, \ldots \qquad (11)$$

équidivisibles avec A lors de la division avec reste par m. Choisissons un procédé de construction de la suite (11) tel

que chacun de ses termes supérieur ou égal à m en valeur absolue soit suivi d'au moins un autre. Si le dernier terme de (11) est nul, A est divisible par m, et, dans le cas contraire, A ne l'est pas.

Appelons *caractère de divisibilité* par m tout procédé de construction de la suite (11).

Problème 40. Montrer que tout caractère de congruence modulo m est un caractère de divisibilité par m.

Il est évident que les caractères de divisibilité doivent satisfaire aux mêmes conditions que ceux de la congruence, c'est-à-dire qu'ils doivent être définis, universels et efficaces.

On vérifie aisément (nous-en laissons le soin au lecteur) qu'à l'aide de toute fonction $f(x)$ satisfaisant aux conditions a)-c) du n° 2 et à la condition

d*) si $f(x)$ a un sens, les nombres x et $f(x)$ sont équidivisibles par m;

on peut établir le caractère de divisibilité par m exactement de la même façon qu'on a établi le caractère de congruence modulo m pour toute fonction satisfaisant aux conditions a)-c), d*).

Trouvons quelques caractères de divisibilité.

Conformément au théorème 16, il suffit de savoir déterminer la divisibilité par les nombres de la forme p^α (la puissance d'un nombre premier).

10. CARACTÈRE DE DIVISIBILITÉ PAR 7. Soit A un nombre naturel. Représentons-le sous la forme $10a + b$, $0 \leqslant b < 10$, comme nous l'avons déjà fait précédemment. Posons

$$f_3(A) = \begin{cases} a - 2b \text{ si } A \geqslant 19, \\ \text{reste de la division de } A \text{ par 7 si } 7 \leqslant A < 19, \\ \text{n'est pas définie si } A < 7. \end{cases}$$

Problème 41. Vérifier que les conditions a)-c) et d*) sont remplies pour la fonction $f_3(A)$.

La fonction $f_3(A)$ nous donne un certain caractère de divisibilité par 7: le nombre $10a + b$ $(0 \leqslant b < 10)$ se divise par 7 si, et seulement si, le nombre $a - 2b$ est divisible par 7; on vérifie de nouveau par le même procédé que le nombre obtenu est divisible par 7, etc.

Problème 42. Montrer que le caractère de divisibilité par 7 obtenu n'est pas un caractère de congruence modulo 7.

11. CARACTÈRE DE DIVISIBILITÉ PAR 13. Représentons le nombre naturel A sous la forme $10a + b$ et posons

$$f_4(A) = \begin{cases} a + 4b \text{ si } A \geqslant 40, \\ \text{reste de la division de } A \text{ par } 13 \text{ si } 13 \leqslant A < 40, \\ \text{n'est pas définie si } A < 13. \end{cases}$$

Problème 43. Vérifier que les conditions a)-c) et d*) sont vérifiées par la fonction $f_4(x)$ et énoncer le caractère de divisibilité par 13 obtenu.

Problème 44. On remplace, dans la définition de la fonction f_4, 40 par un nombre inférieur. Quel en sera le résultat?

Problème 45. Par analogie avec les caractères de divisibilité par 7 et 13 établis précédemment, établir des caractères analogues de divisibilité par 17, 19, 23, 29 et 31.

Problème 46. Etablir deux caractères de divisibilité par 49.

12. Aux numéros précédents du présent paragraphe nous nous sommes familiarisés avec un grand nombre de caractères de congruence modulo m et de divisibilité. En établissant ces caractères on veut en général obtenir des algorithmes commodes pour trouver les restes de divisions par certains nombres définis (caractères de congruence) ou des algorithmes permettant de découvrir si ces restes sont nuls ou non (caractères de divisibilité). Dans quelle mesure ce but a-t-il été atteint?

Certains caractères de congruence, par exemple pour le module 2, 3, 5 et 10, se sont effectivement avérés très pratiques et commodes. Quant à certains autres caractères, leur application exige des calculs plus ou moins laborieux.

On a donc intérêt à chercher et à appliquer les caractères de divisibilité et de congruence modulo m dont l'utilisation conduit au but visé par les voies les plus simples possible.

L'une des difficultés auxquelles on se heurte en l'occurrence est de devoir évaluer numériquement la simplicité (ou, au contraire, la complexité) de l'application de tel ou tel caractère. On peut en qualité d'une telle caractéristique numérique prendre, par exemple, le nombre des opérations arithmétiques à effectuer sur des nombres à un chiffre quand on applique un caractère donné à tel ou tel nombre.

Malheureusement, une telle caractéristique de l'ampleur des calculs dépend dans une grande mesure des particularités du nombre dont il s'agit de vérifier la divisibilité.

Ainsi, on s'aperçoit sans peine que le reste de la division de 31 025 par 8 est 1. Il suffit à cet effet de trouver le reste fourni par la division de 25 par 8. Mais pour trouver le reste de la division du nombre 30 525 par 8, il faut diviser avec reste 525 par 8, ce qui exige un nombre de calculs supérieur (peu importe qu'on les fasse mentalement ou par écrit).

En qualité d'autre exemple, considérons le caractère de congruence modulo 37 (voir problème 35). Le reste de la division du nombre 11 014 023 par 37 est trouvé en ajoutant 10, 14 et 23 et en divisant la somme ainsi obtenue par 37. Ce reste, on le voit aisément, est égal à 10. Cependant, peu nombreux sont ceux qui sont capables d'appliquer mentalement ce caractère au nombre 782 639 485.

Aussi doit-on, quand il s'agit d'évaluer la commodité des caractères de divisibilité et de congruence modulo m, faire abstraction des cas concrets pour évaluer les possibilités de chaque caractère « en moyenne ». En adoptant une telle approche, on peut espérer pouvoir établir avec précision le degré de complexité du caractère considéré, voire

trouver le caractère le plus avantageux. Malheureusement, la place nous manque pour développer cet aspect de la question.

13. Tous les caractères de congruence modulo *m* et de divisibilité établis précédemment paraissent quelque peu artificiels, et on peut même penser que ces caractères ou tout au moins certains d'entre eux ont été trouvés par hasard ou bien à l'issue d'essais. En réalité il n'en est rien. Il existe en effet des procédés pour établir les caractères de congruence modulo *m* et de divisibilité par *m* pour un *m* donné à l'avance qui sont alors appelés *caractères généraux*.

Les caractères généraux de divisibilité sont des *procédés* qui permettent d'obtenir des caractères concrets. Aussi peut-on considérer comme étant des caractères concrets de divisibilité les résultats auxquels conduisent les caractères généraux. De ce point de vue, les caractères généraux sont aux caractères concrets ce qu'un caractère concret est au résultat de son application à un certain nombre, c'est-à-dire au reste de la division d'un nombre donné *a* par un nombre donné *m*.

Les caractères généraux de divisibilité et de congruence modulo *m* rappellent des algorithmes, d'ailleurs assez particuliers: ils doivent avoir pour résultat de nouveaux algorithmes, à savoir des caractères concrets.

Cependant, avant de parler de caractères généraux de divisibilité et de congruence modulo *m* comme d'algorithmes, nous devons nous assurer qu'ils sont définis, universels et efficaces.

Pour être plus explicite, on doit, quand on indique un caractère général de divisibilité (de même qu'un caractère général de congruence modulo *m*), s'assurer qu'il vérifie les conditions suivantes. Premièrement, il doit réellement fournir, pour tout nombre *m*, un caractère de divisibilité par *m* (ou de congruence modulo *m*). Il doit pour ainsi dire « transformer » chaque nombre naturel *m* en un caractère correspondant. C'est précisément en cela que consiste son *effica-*

cité. Deuxièmement, le caractère général doit être *défini*, c'est-à-dire qu'appliqué à un nombre m donné, il doit conduire d'une manière bien définie à un caractère concret de divisibilité par m (ou de congruence modulo m) bien défini. Pour finir, le caractère doit être *universel*, c'est-à-dire vraiment général, et fournir les caractères de divisibilité ou de congruence pour tout nombre naturel donné à l'avance.

Dans ce sens, le procédé de détermination du caractère de congruence modulo m décrit au n° 2, de même que le procédé conduisant aux caractères de divisibilité (n° 6) ne sont pas des caractères généraux, car le processus qui consiste à indiquer les fonctions satisfaisant aux conditions voulues n'est encore ni défini, ni universel, ni efficace.

En effet, ces procédés ne garantissent nullement que la fonction voulue sera trouvée, donc ils ne sont pas efficaces. De plus, quand bien même la fonction nécessaire existerait, on peut y arriver par des voies différentes, sans parler du fait qu'il peut y en avoir plus d'une. Donc, ces procédés ne sont pas définis. Enfin, ils ne sont pas non plus universels, car il se peut que pour certains nombres on ne soit pas en mesure de trouver les fonctions nécessaires. En tout cas, le procédé même ne nous donne aucune indication à cet égard. De la sorte, pour que le processus décrit soit un algorithme, il doit être complété d'indications précises garantissant la construction d'une fonction f_m bien définie pour chaque nombre m concret.

Ce problème d'algorithmisation de l'établissement de caractères de divisibilité n'est pas bien difficile à résoudre. Quant aux caractères de divisibilité généraux, ils sont connus depuis longtemps.

Nous avons établi un tel caractère général de congruence modulo m au n° 11 du § 1 lorsque nous avons traité la question de la division avec reste. On peut le formuler ainsi : on fait correspondre à tout entier positif m un processus de soustractions successives de ce nombre jusqu'à ce qu'on obtienne un nombre inférieur à m (voir la dernière phrase

du nº 1 du présent paragraphe). Il est évident qu'une telle correspondance possède les propriétés voulues: elle est définie (on sait exactement que l'on fait correspondre au nombre *m* le processus de soustractions successives de *m*), universelle (on peut tenter de faire correspondre le processus de soustractions successives à tout *m*) et efficace (une telle tentative aboutira sûrement). Cependant, en pratique, ce caractère général de congruence modulo *m* ne sert pas à grand-chose.

Un certain perfectionnement du caractère général de congruence, fondé sur des soustractions successives, nous conduit au procédé usuel de division des nombres entiers, qu'on peut également considérer comme étant un caractère général de congruence modulo *m*. Il n'est pas superflu de rappeler que tel est précisément le caractère dont on se sert dans la plupart des cas pour trouver le reste d'une division. Le raisonnement se fait selon le schéma suivant, que nous reproduisons en deux variantes: en langage ordinaire et en langage d'algorithmes.

En langage ordinaire	En langage d'algorithmes
1. Soit à trouver le reste de la division d'un nombre donné *a* par un nombre donné *m* ;	Le caractère général de congruence commence la transformation du nombre *m* ;
2. je dois diviser par *m* ;	le caractère général «fournit» le résultat du traitement du nombre *m* : le caractère concret de congruence modulo *m*, qui est la division directe par *m* ;
3. je commence à diviser *a* par *m*...	le caractère concret obtenu commence le traitement du nombre *a* ;
4. ...j'effectue la division et je trouve un reste.	le caractère concret conduit au but : au reste de la division de *a* par *m*.

Les trois premiers pas des raisonnements sont on ne peut plus simples, aussi ne faut-il pas s'étonner que le quatrième, qui consiste à effectuer la division, s'avère si laborieux. L'élaboration de caractères généraux de congruence modulo m et de divisibilité a précisément pour but de faciliter le quatrième pas en perfectionnant le deuxième. C'est ce qu'on a généralement en vue quand on parle des caractères généraux de divisibilité et de congruence modulo m.

14. Du point de vue historique, le premier caractère général de divisibilité (de congruence modulo m, pour être plus précis) fut proposé par Pascal dès le milieu du XVII[e] siècle. Le voici.

Soit m un nombre naturel. Formons la suite de nombres

$$r_1, r_2, r_3, \ldots, \qquad (12)$$

en posant

r_1	égal au reste	de la division	de	10 par m,
r_2	»	»	»	$10\, r_1$ par m,
r_3	»	»	»	$10\, r_2$ par m,

etc.

Mettons maintenant un nombre naturel arbitraire A sous la forme

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10 a_1 + a_0$$

et définissons la fonction

$$F_m(a) = \begin{cases} a_0 + r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \text{ si } 10^n \geqslant m, \\ \text{reste de la division de } A \text{ par } m \text{ si } 10^n < m \leqslant A, \\ \text{n'est pas définie si } A < m. \end{cases}$$

Problème 47. Vérifier que pour n'importe quel m la fonction F_m satisfait aux conditions a)-d).

Ainsi, nous avons établi le caractère de congruence modulo m, m étant un nombre quelconque, c'est-à-dire un caractère général.

Problème 48. Enoncer les caractères de congruence, obtenus à partir du caractère général de Pascal, pour les modules suivants:

a) 2, 5 et 10;
b) 4, 20 et 25;
c) 3 et 9;
d) 11; e) 7.

Problème 49. Supposons que dans la suite (12) r_1 soit le reste de la division de 100 par m, r_2 celui de la division de 100 r_1 par m, r_2 celui de la division de 100 r_2 par m, etc. En déduire un caractère général de congruence modulo m analogue au caractère de Pascal.

15. Au n° 12, il a été question du degré de complexité de différents caractères de divisibilité (ou de congruence) pour un nombre donné. Comme un caractère général de divisibilité doit nous fournir des caractères de divisibilité par n'importe quel nombre naturel, il n'est pas surprenant qu'il puisse pour des nombres différents conduire à des caractères de divisibilité de qualités très diverses.

Ainsi, parallèlement à des caractères de congruence modulo 3 et 11 tout à fait satisfaisants, le caractère général de Pascal fournit un caractère de congruence modulo 7 très laborieux et incommode (voir problème 48,e)).

En conséquence, on peut, à propos des caractères généraux de divisibilité et de congruence modulo m, formuler des considérations analogues à celles que nous avons exposées au n° 12 lors de l'examen des qualités des caractères concrets. On doit donc considérer que le meilleur caractère général de divisibilité (de congruence) est celui qui, appliqué à tout entier positif m donné à l'avance, fournit le meilleur caractère de divisibilité par m (de congruence modulo m). Signalons qu'on n'est pas encore parvenu, tant s'en faut, non seulement à résoudre le problème de la recherche du meilleur caractère général de divisibilité, mais même à poser ce problème avec rigueur.

§ 4 DIVISIBILITÉ DES PUISSANCES

1. La question de la divisibilité des puissances se ramène au fond à celle de la divisibilité d'un certain produit, plus précisément d'un produit de plusieurs facteurs égaux. Aussi peut-on également résoudre cette question sur la base des résultats du § 2. Cependant, dans le cas des exposants élevés, la diminution de la base de la puissance ne permet pas de trouver d'emblée le reste de la division de la puissance, ce qui nous oblige à recourir à des procédés quelque peu artificiels (voir exemples du n° 2, § 2). De plus, en établissant les caractères généraux de divisibilité, nous avons calculé les restes des divisions des puissances successives du nombre 10 par m. Bien que par lui-même ce processus soit assez simple, il ne révèle pas l'existence d'une régularité quelconque dans la suite (12) et ne nous permet pas de prendre l'exposant k tel que tous ces restes soient suffisamment petits (or, la chose est possible ; bien plus, il s'avère qu'on peut choisir k tel que tous ces restes soient égaux à l'unité).

Tout ceci nous oblige à étudier plus en détail la divisibilité des puissances.

2. Elargissons quelque peu nos connaissances dans le domaine de la théorie des nombres.

● THÉORÈME 19 (théorème de Fermat). *L'expression $a^p - a$ dans laquelle p est un nombre premier est divisible par p.*

Il ne faut pas confondre ce théorème avec le dernier théorème de Fermat qui affirme que pour un entier $n > 2$ il n'existe pas de nombres entiers a, b et c tels que $a^n + b^n = c^n$. Malgré de multiples tentatives, personne n'a encore ni démontré ni infirmé le dernier théorème de Fermat.

● CONSÉQUENCE. Si p est premier et que a ne soit pas divisible par p, $a^p - 1$ est divisible par p.

Problème 50. Citer un exemple prouvant que ni le théorème 20 ni sa conséquence ne sont en général valables pour un p composé.

Problème 51. Démontrer le théorème de Fermat en s'appuyant sur le résultat du problème 26.

Soit

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \quad (13)$$

la décomposition canonique d'un nombre naturel m. Posons

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha - 1}(p_k - 1). \quad (14)$$

Les formules (13) et (14) font correspondre à chaque nombre naturel m un nombre $\varphi(m)$ bien défini, de sorte qu'on peut parler de la fonction φ d'une variable naturelle.

● DÉFINITION. La fonction $\varphi(m)$ définie ci-dessus est appelée *fonction d'Euler.*

La fonction d'Euler joue un rôle exceptionnel dans de nombreuses questions de la théorie des nombres. Nous en indiquons quelques applications.

● THÉORÈME 20. *Pour des nombres m_1 et m_2 premiers entre eux, on a l'égalité*

$$\varphi(m_1 m_2) = \varphi(m_1)\, \varphi(m_2).$$

Problème 52. Calculer $\varphi(12)$, $\varphi(120)$, $\varphi(1000)$.

Problème 53. Déterminer tous les nombres m pour lesquels

a) $\varphi(m) = 10$,

b) $\varphi(m) = 8$.

Problème 54. Démontrer qu'il n'existe pas de nombre m tel que $\varphi(m) = 14$.

Problème 55. Montrer que $\varphi(m)$ est égale au nombre des nombres naturels premiers avec m et inférieurs à m. Cette propriété de la fonction d'Euler s'avère extrêmement impor-

tante, et on l'adopte souvent comme définition de cette fonction.

● THÉORÈME 21 (théorème d'Euler). $a^{\varphi(m)}-1$ *est divisible par m si a et m sont premiers entre eux.*

3. A l'aide des théorèmes démontrés, établissons quelques caractères généraux de divisibilité et de congruence modulo m.

Fixons un m naturel et représentons A sous la forme

$$A=a_0+a_1 10^{\varphi(m)}+a_2 10^{2\varphi(m)}+\ldots+a_k 10^{k\varphi(m)},$$

où

$$0\leqslant a_0,\ a_1,\ a_2,\ \ldots,\ a_k\leqslant 10^{\varphi(m)},$$

c'est-à-dire que les nombres a_i ($i=0, 1, \ldots, k$) ont $\varphi(m)$ chiffres.

Comme on le vérifie aisément, la fonction F

$$F(A)=\begin{cases} a_0+a_1+\ldots+a_k \text{ si } A\geqslant 10^{\varphi(m)}, \\ \text{reste de la division de } A \text{ par } m \text{ si } m\leqslant A<10^{\varphi(m)}, \\ \text{n'est pas définie si } A<m \end{cases}$$

définit un certain caractère général de congruence modulo m.

Problème 56. Vérifier cette circonstance.

● THÉORÈME 22. *Si a et m sont premiers entre eux et* k_1 *et* k_2 *sont congrus modulo* $\varphi(m)$, a^{k_1} *et* a^{k_2} *sont congrus modulo m.*

Problème 57. Démontrer que $n^{13}-n \vdots 2730$.

4. Dans de nombreux cas, le caractère général établi ci-dessus n'est pas assez avantageux, car le nombre $\varphi(m)$ peut en général s'avérer assez grand. Aussi doit-on, quand on utilise ce caractère, d'une part, additionner de grands nombres et, d'autre part, diviser les nombres de $\varphi(m)$ chiffres

directement par m (ou bien se servir de quelque autre caractère de divisibilité ou de congruence modulo m). On a donc intérêt à essayer de substituer à $\varphi(m)$ un exposant plus petit, ce qui, dans certains cas, s'avère possible. Ainsi, pour $m = 37$, on peut, au lieu de $\varphi(m) = 36$, prendre 3, car le reste de la division de 1000 par 37 est 1; pour $m = 11$, on peut, au lieu de $\varphi(m) = 10$, prendre 2, etc.

● DÉFINITION. Le plus petit nombre δ tel que a^{δ} divisé par m donne 1 pour reste s'appelle l'*exposant* auquel appartient le nombre a lors de la division avec reste par m.

On donne plus souvent à ce nombre le nom d'exposant auquel appartient le nombre a *modulo* m.

Il est évident que, quels que soient les nombres a et m premiers entre eux, l'exposant auquel appartient a modulo m ne dépasse pas $\varphi(m)$. Aussi peut-on substituer cet exposant à $\varphi(m)$ dans l'énoncé du caractère général de divisibilité du n° 3.

Problème 58. Modifier le caractère général de divisibilité qu'on vient d'établir en remplaçant $\varphi(m)$ par l'exposant auquel appartient 10 modulo m.

5. Les applications de la fonction d'Euler et du théorème d'Euler ne se bornent pas aux caractères de divisibilité. On peut s'en servir pour résoudre des équations en nombres entiers.

● THÉORÈME 23. *Si les nombres a et b sont premiers entre eux, l'équation*

$$ax + by = c \tag{15}$$

admet toujours des solutions entières qui sont tous les couples de nombres (x_t, y_t), où

$$x_t = ca^{\varphi(b)-1} + bt,$$

$$y_t = c\,\frac{1 - a^{\varphi(b)}}{b} - at$$

(*t étant un nombre entier quelconque*).

Problème 59. Démontrer un théorème analogue au théorème 23 sans supposer les nombres a et b premiers entre eux.

Problème 60. Trouver un procédé de résolution des équations de la forme (15) à l'aide des nombres entiers sur la base du résultat du problème 29.

Problème 61. Trouver les solutions entières des équations

a) $5x + 7y = 9$,

b) $25x + 13y = 8$.

6. THÉORÈME 24. *Si m et 10 sont premiers entre eux et que k soit congru à $10^{\varphi(m)-1}$ modulo m, les nombres $10a + b$ et $a + kb$ sont équidivisibles par m.*

On peut, en s'appuyant sur ce théorème, établir un caractère général de divisibilité. Soit k' le reste modulo m de $10^{\varphi(m)-1}$. Représentons un nombre A quelconque sous la forme $10a + b$ $(0 \leqslant b < 10)$ et posons

$$F(A) = \begin{cases} a + k'b \text{ si } A > a + k'b, \\ \text{reste de la division de } A \text{ par } m \text{ si } m \leqslant A < \\ \qquad\qquad\qquad\qquad < a + k'b, \\ \text{n'est pas définie si } A < m. \end{cases}$$

Si k' est grand (proche de m), on a intérêt à lui substituer $k' - m$ dans l'énoncé du caractère correspondant.

Problème 62. Vérifier que les conditions a)-b) et d*) sont remplies pour la fonction F.

Problème 63. Compte tenu du caractère général de divisibilité que nous venons d'établir, déduire les caractères de divisibilité par 17, 19, 27, 29, 31 et 49.

Problème 64. Etablir un caractère de divisibilité analogue en représentant un nombre naturel quelconque sous la forme $100a + b$ $(0 \leqslant b < 100)$ et en déduire les caractères de divisibilité par 17, 43, 49, 67, 101, 199.

DÉMONSTRATIONS DES THÉORÈMES

1. Il suffit de noter que $a = a \cdot 1$.
2. Par hypothèse on peut choisir d_1 et d_2 tels que $a = bd_1$ et $b = cd_2$. Mais dans ce cas, $a = cd_1d_2$, i.e. $d \vdots c$.
3. Nous avons $a = bc_1$ et $b = ac_2$, d'où $a = ac_1c_2$, i.e. $c_1c_2 = 1$. Comme par hypothèse les nombres c_1 et c_2 sont entiers, on a soit $c_1 = c_2 = 1$, soit $c_1 = c_2 = -1$. Dans le premier cas, $a = b$, dans le second, $a = -b$.
4. Soit $a = bc$. Si $|c| \geqslant 1$, étant donné que $|b| > |a|$, on doit également avoir $|bc| \geqslant |a|$, ce qui est contraire à notre supposition, donc $|c| < 1$, et comme par hypothèse le nombre c est entier, on doit avoir $c = 0$ et, partant, $a = 0$.
5. Il découle évidemment de $a = bc$ que $|a| = |b||c|$ et inversement, les nombres c et $|c|$ étant simultanément entiers ou non.
6. En effet, soit

$$\begin{aligned} a_1 &= bc_1, \\ a_2 &= bc_2, \\ &\dots\dots\dots \\ a_n &= bc_n, \end{aligned}$$

où tous les nombres $c_1, c_2, \ldots, c_n$ sont entiers. En ajoutant terme à terme toutes ces égalités, on a

$$a_1 + a_2 + \ldots + a_n = b(c_1 + c_2 + \ldots + c_n).$$

La présence d'un nombre entier entre parenthèses apporte la preuve nécessaire.
8. Raisonnons par l'absurde. Supposons que les nombres premiers soient en nombre fini et qu'on puisse donc les écrire comme suit :

$$p_1, p_2, \ldots, p_n. \tag{16}$$

Désignons par P le produit de tous ces nombres et examinons la différence $P - 1$. Cette différence est supérieure

à chacun des nombres premiers de (16) et ne peut donc être un nombre premier. En conséquence, cette différence est divisible par un seul nombre premier p_k au moins. Mais P est lui aussi divisible par p_k. Donc, en vertu de la conséquence du théorème 6, on doit également avoir $1 \vdots p_k$, d'où il découle que $p_k = 1$, ce qui est contraire au fait que le nombre p_k est premier (voir p. 25).

Cette démonstration de l'infinitude de l'ensemble des nombres premiers a été trouvée par Euclide (IVe siècle av. J.-C.).

9. Si les nombres a et p sont premiers entre eux, le théorème est démontré. S'ils ne le sont pas, ils sont tous deux divisibles par un même nombre différent de l'unité. Etant donné que p est un nombre premier, ce nombre ne peut être que p lui-même. Donc, dans ce cas, $a \vdots p$, C.Q.F.D.

10. Divisant M par m avec reste, on a

$$M = mq + r,$$

où $0 \leqslant r < m$. Etant donné que M et m sont divisibles par a et b, en vertu de la conséquence du théorème 6, le nombre r lui aussi doit admettre a et b pour diviseurs et être donc un multiple commun à ces nombres. Mais $r < m$, et m est le plus petit commun multiple positif de a et b. r ne peut donc être un nombre positif, ce qui fait que $r = 0$. C'est pourquoi $M \vdots m$.

11. Supposons que les nombres a et b soient premiers entre eux et que m soit leur plus petit commun multiple. Comme $ab \vdots a$ et $ab \vdots b$, d'après le théorème précédent $ab \vdots m$. Soit $ab = mk$. Posons $m = ac$. Dans ce cas, $ab = ack$, c'est-à-dire $b = ck$, de sorte que $b \vdots k$. On s'assure exactement de la même façon que $a \vdots k$. Comme par hypothèse les nombres a et b sont premiers entre eux, on doit avoir $k = 1$, ce qui signifie précisément que $m = ab$.

12. Désignons par m le plus petit commun multiple des nombres b et c. D'après le théorème précédent, $m = bc$. Ensuite, par hypothèse $ab \vdots c$; de plus, il est évident que

$ab \vdots b$. Donc, d'après le théorème 10, $ab \vdots bc$, c'est-à-dire $ab = bck$ ou, en simplifiant, $a = ck$, C.Q.F.D.

13. La démonstration se fait par récurrence sur le nombre de facteurs. S'il n'y en a qu'un, le théorème est trivial. Supposons le théorème démontré pour n'importe quel produit de n facteurs. Soit $a_1a_2 \ldots a_na_{n+1} \vdots p$. Désignons $a_1a_2 \ldots a_n$ par A. On a alors $Aa_{n+1} \vdots p$. Si $a_{n+1} \vdots p$, le théorème est démontré, sinon, d'après le théorème 9, a_{n+1} et p sont premiers entre eux. Mais alors, en vertu de ce qui précède, $A \vdots p$. Comme A est un produit de n facteurs, par hypothèse de récurrence, l'un d'eux doit être divisible par p. Le théorème est ainsi prouvé.

● CONSÉQUENCE. Toute la fraction représente un nombre entier (son numérateur se divise par son dénominateur). Nous considérerons que le numérateur est un produit de deux facteurs: p et $1 \cdot 2 \ldots (p-1) = (p-1)!$

Aucun des facteurs du dénominateur de la fraction n'est divisible par p. En conséquence, d'après le théorème précédent, le dénominateur tout entier n'est pas non plus divisible par p. Mais alors, en vertu du théorème 9, le dénominateur est premier avec p. Aussi le deuxième facteur du numérateur doit-il être divisible par le dénominateur. En désignant le quotient de cette division par q, il vient $C_p^k =$ $= pq$, C.Q.F.D.

14. Prouvons d'abord qu'on *peut* décomposer n'importe quel nombre différent de l'unité en facteurs premiers. Supposons que tous les nombres inférieurs à N admettent une telle décomposition. Si N est premier, il se décompose automatiquement en un produit de facteurs premiers (qui ne comprend qu'un seul facteur, à savoir le nombre N lui-même), et le théorème est prouvé. Supposons maintenant que N soit un nombre composé, N_1 un certain diviseur de N différent tant de N que de l'unité et N_2 le quotient de la division de N par N_1. Dans ce cas, $N = N_1N_2$, et comme on le vérifie aisément, $1 < N_2 < N$. Etant donné que N_1 et

N_2 sont inférieurs à N^2, dans notre supposition, ils se décomposent en facteurs premiers. Soient $N_1 = p_1p_2 \ldots p_k$ et $N_2 = q_1q_2 \ldots q_l$ ces décompositions. Dans ce cas, $p_1p_2 \ldots p_kq_1q_2 \ldots q_l$ est la décomposition cherchée du nombre N. Nous avons ainsi prouvé que la décomposition est possible.

Passons à la démonstration de l'*unicité* de la décomposition. Soient $p_1p_2 \ldots p_k$ et $q_1q_2 \ldots q_l$ deux décompositions du nombre N en facteurs premiers. Il est évident que

$$p_1p_2 \ldots p_k = q_1q_2 \ldots q_l. \tag{17}$$

Etant donné que $q_1q_2 \ldots q_l$ est divisible par p_1, d'après le théorème précédent, l'un au moins des nombres $q_1, q_2, \ldots, q_l$ est divisible par p_1. Soit $q_1 \vdots p_1$ (le fait d'avoir supposé précisément le premier facteur du deuxième membre de (17) divisible par p_1 n'impose aucune condition supplémentaire, car on est en droit d'intervertir les facteurs et de noter q_1 le facteur qui est divisible par p_1). Comme le nombre q_1 est premier, cela n'est possible que pour $p_1 = q_1$. En divisant (17) par p_1, on a

$$p_2p_3 \ldots p_k = q_2q_3 \ldots q_l. \tag{18}$$

Par analogie avec le cas précédent, on constate que l'un des nombres $q_2, q_3, \ldots, q_l$ (q_2 par exemple) est divisible par p_2, ce qui fait que $p_2 = q_2$. En divisant l'égalité (18) par p_2, nous diminuons encore d'une unité le nombre des facteurs de ses membres. Nous pouvons apparemment poursuivre l'opération jusqu'à ce que l'un des produits soit égal à l'unité. Supposons que le premier à l'être soit le produit du premier membre de (17). Le produit du deuxième membre de (17) doit lui aussi se simplifier entièrement, sinon on obtiendrait une égalité de la forme

$$1 = q_{k+1} \ldots q_l$$

qui est impossible, car l'unité n'est divisible par aucun

nombre premier. On a également

$$p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_k = q_k.$$

Le théorème est entièrement démontré.

15. Soient $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ et $q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$ les décompositions canoniques respectives des nombres a et b et d un certain diviseur commun à ces nombres. Si $d \neq 1$, d est divisible par un nombre premier p. Dans ce cas, d'après le théorème 3, $a \vdots p$ et $b \vdots p$, de sorte que p se trouve tant parmi les nombres $p_1, p_2, \ldots, p_k$ que parmi les nombres $q_1, q_2, \ldots, q_l$. Aussi au moins l'un des nombres premiers faisant partie de la décomposition canonique de a figure-t-il dans la décomposition canonique de b.

Par contre, si a et b sont premiers entre eux et que p fasse partie de la décomposition canonique de a, b n'est pas divisible par p, de sorte que p ne peut se trouver dans la décomposition canonique de b.

16. *Nécessité.* Etant donné que $a \vdots p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$, on tire la condition nécessaire de $b \vdots a$ en s'en référant tout simplement au théorème 2.

La *suffisance* se démontre par récurrence. La divisibilité $b \vdots p_1^{\alpha_1}$ fait partie des conditions. Supposons que nous ayons déjà établi que

$$b \vdots p_1^{\alpha_1} \ldots p_l^{\alpha_l} \quad (1 \leqslant l < k).$$

De plus, nous avons à notre disposition la divisibilité $b \vdots p_{l+1}^{\alpha_{l+1}}$. Comme, d'après le théorème précédent, les nombres $p_1^{\alpha_1} \ldots p_l^{\alpha_l}$ et $p_{l+1}^{\alpha_{l+1}}$ sont premiers entre eux, nous pouvons appliquer la conséquence du théoreme 11 et écrire

$$b \vdots p_1^{\alpha_1} \ldots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}},$$

ce qui achève la démonstration par récurrence.

17. *Nécessité.* Soit

$$a = mq_1 + r_1 \quad (0 \leqslant r_1 < m), \tag{19}$$
$$b = mq_2 + r_2 \quad (0 \leqslant r_2 < m). \tag{20}$$

Etant donné que a et b divisés par m donnent le même reste, on a $r_1 = r_2$. Donc

$$a - b = m(q_1 - q_2),$$

c.-à-d. $a - b \,\vdots\, m$.

Suffisance. Soit $a - b \,\vdots\, m$. En divisant avec reste a et b par m, on obtient (19) et (20). On a alors

$$a - b = m(q_1 - q_2) + r_1 - r_2,$$

c.-à-d.

$$(a - b) - m(q_1 - q_2) = r_1 - r_2.$$

D'après le théorème 6, $r_1 - r_2 \,\vdots\, m$. Mais $|r_1 - r_2| < m$. Donc, d'après le théorème 4, $r_1 - r_2 = 0$, ou $r_1 = r_2$, C.Q.F.D.

18. L'hypothèse nous donne en vertu du théorème 16:

$$\left.\begin{array}{l} a_1 = b_1 + mq_1, \\ a_2 = b_2 + mq_2, \\ \cdots\cdots\cdots\cdots \\ a_n = b_n + mq_n. \end{array}\right\} \tag{21}$$

Ajoutant terme à terme ces égalités nous obtenons après de simples transformations

$$(a_1 + a_2 + \ldots + a_n) - (b_1 + b_2 + \ldots + b_n) = \\ = m(q_1 + q_2 + \ldots + q_n),$$

ce qui, d'après le théorème 17, prouve précisément que les sommes divisées par m donnent les mêmes restes.

Pour démontrer l'égalité des restes dans le cas des produits, notons l'identité suivante

$$(k + bm)(p + qm) = kp + (pq + lp + lqm)\,m$$

dont il découle que le produit de deux nombres de la forme $a + bm$ est lui-même un nombre de cette forme. Aussi, en raisonnant par récurrence, on s'assure que le produit de nombres de la forme $a + bm$ en nombre quelconque est un nombre de cette même forme.

En multipliant maintenant membre à membre toutes les égalités (21) et en appliquant au deuxième membre le raisonnement ci-dessus, on obtient

$$a_1a_2 \ldots a_n = b_1b_2 \ldots b_n + mt,$$

où t est un certain entier. Nous avons ainsi démontré que les produits donnent le même reste.

19. La démonstration se fait par récurrence sur a. Pour $a = 1$, on a

$$a^p - a = 1 - 1 = 0$$

et $0 \vdots p$.

Supposons que $a^p - a$ soit divisible par p et démontrons que $(a + 1)^p - (a + 1)$ l'est également. En effet, en décomposant $(a + 1)^p$ d'après la formule du binôme de Newton, on a

$$(a+1)^p-(a+1)=a^p+C_p^1a^{p-1}+C_p^2a^{p-2}+\ldots+ \\ +C_p^{p-1}a+1-a-1=a^p-a+C_p^1a^{p-1}+ \\ +C_p^2a^{p-2}+\ldots+C_p^{p-1}a. \qquad (22)$$

$a^p - a$ est divisible par p par supposition. D'après la conséquence du théorème 13, C_p^k $(1 \leqslant k \leqslant p - 1)$ est également divisible par p. Par conséquent, chaque terme de la somme (22) est divisible par p et, partant (d'après le théorème 6), la somme aussi.

Le raisonnement est terminé, et tout le théorème est démontré.

● CONSÉQUENCE. D'après le théorème de Fermat

$$a^p - a = a\,(a^{p-1} - 1) \vdots p.$$

Si a n'est pas divisible par p, d'après le théorème 13, $a^{p-1}-1$ doit l'être.

20. Soit $m_1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ et $m_2 = q_1^{\beta_1} \ldots q_l^{\beta_l}$. D'après le théorème 15, aucun des nombres $p_1, \ldots, p_k$ ne coïncide avec aucun des nombres $q_1, \ldots, q_l$. Donc la décomposition canonique de m_1m_2 est $p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\beta_1} \ldots q_l^{\beta_l}$, c'est pourquoi

$$\varphi(m_1m_2) = p_1^{\alpha_1-1}(p_1-1) \ldots p_k^{\alpha_k-1}(p_k-1) q_1^{\beta_1-1}(q_1-1) \ldots$$
$$\ldots q_l^{\beta_l-1}(q_l-1),$$

c'est-à-dire

$$\varphi(m_1m_2) = \varphi(m_1)\,\varphi(m_2).$$

21. Démontrons d'abord par récurrence sur α que $a^{p^{\alpha-1}(p-1)}-1$ est divisible par p^α. Pour $\alpha = 1$, la proposition est évidemment la conséquence du théorème de Fermat, dont nous avons déjà établi la validité.

Supposons maintenant que $a^{p^{\alpha-1}(p-1)}-1 \vdots p^\alpha$ et considérons l'expression $a^{p^\alpha(p-1)}-1$. Il s'agit de démontrer qu'elle est divisible par $p^{\alpha+1}$. Mais

$$a^{p^\alpha(p-1)}-1 = (a^{p^{\alpha-1}(p-1)})^p - 1.$$

Comme, par supposition, $a^{p^{\alpha-1}(p-1)}-1$ est divisible par p^α, le nombre $a^{p^{\alpha-1}(p-1)}$ se présente sous la forme $Np^\alpha + 1$. Donc

$$a^{p^\alpha(p-1)}-1 = (Np^\alpha+1)^p - 1,$$

c'est-à-dire, d'après la formule du binôme,

$$a^{p^\alpha(p-1)}-1 = N^p p^{\alpha p} + C_p^1 N^{p-1} p^{\alpha(p-1)} + \ldots$$
$$\ldots + C_p^{p-1} N p^\alpha + 1 - 1.$$

Dans la dernière somme, le premier terme est divisible par $p^{\alpha+1}$, car il l'est par $p^{\alpha p}$, et $\alpha p \geqslant \alpha + 1$. Chacun des $p - 1$ termes suivants comprend p affecté d'un exposant au moins égal à α et un coefficient binomial qui, en vertu de la conséquence du théorème 13, est divisible par p. Donc, chacun de ces termes est également divisible par $p^{\alpha+1}$. Enfin, la différence $1-1=0$ peut être négligée. Aussi, d'après le théorème 6, $a^{p^{\alpha}(p-1)} - 1 \vdots p^{\alpha+1}$. Nous avons donc analysé le cas où le nombre m n'a qu'un seul diviseur premier.

Supposons maintenant le théorème d'Euler prouvé pour les exposants m_1 et m_2, les nombres m_1 et m_2 étant premiers entre eux. Démontrons le théorème d'Euler pour l'exposant $m = m_1 m_2$. Si l'on pose ensuite $m_1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ et $m_2 = p_{k+1}^{\alpha_{k+1}}$, nous obtenons le résultat qui achève la démonstration du théorème. Prouvons la proposition énoncée.

Soient a et m des nombres premiers entre eux. Dans ce cas, a est également premier avec m_1. Par conséquent, $a^{\varphi(m_2)}$ est premier avec m_1. Donc, par hypothèse,

$$(a^{\varphi(m_2)})^{\varphi(m_1)} - 1 = a^{\varphi(m_1)\varphi(m_2)} - 1 = a^{\varphi(m_1 m_2)} - 1 = a^{\varphi(m)} - 1$$

est divisible par m_1. On s'assure exactement de la même manière que $a^{\varphi(m)} - 1$ est divisible par m_2. Etant donné que les nombres m_1 et m_2 sont premiers entre eux, $a^{\varphi(m)} - 1$ est divisible par leur produit, c.-à-d. par m. Le théorème d'Euler est démontré.

22. Soit

$$k_1 = \varphi(m) q_1 + r,$$
$$k_2 = \varphi(m) q_2 + r.$$

Dans ce cas,

$$a^{k_1} = a^{\varphi(m) q_1 + r} = (a^{\varphi(m)})^{q_1} a^r.$$

Selon le théorème d'Euler et le théorème 18, $a^{\varphi(m) q_1} a^r$ est congru à a^r modulo m. On établit de façon analogue qu'il

en est de même des nombres a^{k_2} et a^r. Donc, les nombres a^{k_1} et a^{k_2} sont eux aussi congrus modulo m.

23. Trouvons d'abord au moins une solution (x', y') de cette équation. Il est évident qu'il suffit à cet effet de trouver un nombre x' tel que $ax' - c \vdots b$. D'après le théorème d'Euler, $a^{\varphi(b)} - 1 \vdots b$. Donc, $ca^{\varphi(b)} - c \vdots b$, et on peut en qualité de x' prendre le nombre $ca^{\varphi(b)-1}$.

Supposons maintenant que (x'', y'') soit une autre solution de l'équation $ax + by = c$. Montrons que les nombres x' et x'' divisés par b donnent le même reste. En effet, soit

$$ax' + by' = c,$$
$$ax'' + by'' = c.$$

Soustrayant terme à terme la deuxième égalité de la première, on a

$$a(x' - x'') - b(y' - y'') = 0,$$

d'où $a(x' - x'') \vdots b$. Comme, par hypothèse, a et b sont premiers entre eux, d'après le théorème 12, $x' - x'' \vdots b$, et il ne nous reste qu'à nous en référer au théorème 17.

De la sorte, toutes les valeurs cherchées de x se trouvent parmi les nombres

$$x_t = ca^{\varphi(b)-1} + bt.$$

Mais $ax_t - c \vdots b$, de sorte que si l'on pose

$$y_t = \frac{-ax_t + c}{b} = c\frac{1 - a^{\varphi(b)}}{b} - at,$$

on obtient que tous les couples de nombres x_t et y_t sont solutions de notre équation.

24. Etant donné que les nombres m et 10 sont premiers entre eux, d'après le théorème 15, les nombres $10a + b$ et $(10a + b)\,10^{\varphi(m)-1}$ sont équidivisibles par m. Mais

$$(10a + b)\,10^{\varphi(m)-1} = 10^{\varphi(m)}a + 10^{\varphi(m)-1}b,$$

de sorte que, selon le théorème d'Euler et le théorème 18, $10a + b$ et $a + kb$ sont équidivisibles par m.

SOLUTIONS DES PROBLÈMES

1. $0 = a \cdot 0$ quel que soit a.

2. $a = 1 \cdot a$, donc $a \vdots 1$.

3. Soit $1 \vdots a$, ce qui signifie que $1 = ac$ pour un certain nombre entier c. Il s'ensuit que $|a| \leqslant 1$. Mais comme $a \neq 0$, on doit avoir $a = 1$.

4. Il suffit de choisir n'importe quel $c > 1$ et de poser $b = ac$.

5. On peut, par exemple, prendre $2a$ pour un tel b. Supposons que pour un certain c, $2a \vdots c$ et $c \vdots a$. Cela veut dire qu'on peut choisir d_1 et d_2 tels que $2a = d_1c$ et $c = d_2a$. Il en résulte que $2a = d_1d_2a$ ou, après réduction par a,

$$2 = d_1d_2.$$

Mais pour d_1 et d_2 entiers, une telle égalité n'est possible qu'au cas où l'un de ces nombres est 1 et l'autre 2. Si $d_1 = 1$, on a $c = 2a = b$. Si, par contre, $d_2 = 1$, alors $c = a$.

6. Les démonstrations ne diffèrent en rien de celles dans le cas d'une divisibilité ordinaire.

7. Soit n un nombre fixe supérieur à 1. Posons $a \underset{n}{\vdots} b$ si un entier c peut être tel que $a = bc$ et $c \leqslant n$. La validité des théorèmes analogues aux théorèmes 1, 3 et 4 se vérifie sans peine. Cependant, si nous prenons $a = nb$ et $b = nc$, alors $a \underset{n}{\vdots} b$ et $b \underset{n}{\vdots} c$. Dans ce cas, $a = n^2c$ et, comme $n^2 > n$, la divisibilité $a \underset{n}{\vdots} c$ est impossible. Il en est de même de la divisibilité $a + a \underset{n}{\vdots} b$.

8. a) Soient a_1 et a_2 deux nombres minimaux. En vertu de la dichotomie, on a soit $a_1 \geqslant a_2$, soit $a_2 \geqslant a_1$. Si $a_1 \geqslant a_2$, il résulte de la minimalité de a_1 que $a_1 = a_2$. Si, par contre, $a_2 \geqslant a_1$, $a_1 = a_2$ résulte de la minimalité de a_2.

b) Soient a un nombre quelconque, b_1 et b_2 ses antécédents. En raison de la dichotomie, on doit avoir soit $b_1 \geqslant b_2$, soit $b_2 \geqslant b_1$. Soit, pour fixer les idées, $b_1 \geqslant b_2$. On a $a \geqslant b_1 \geqslant b_2$ et, comme le nombre b_2 précède immédiatement le nombre a, on doit avoir soit $b_1 = a$, soit $b_1 = b_2$. Mais, par hypothèse, $b_1 \neq a$, donc $b_1 = b_2$, ce qui démontre l'unicité.

c) On appelle le *successeur* de a, ou le *suivant* de a, un nombre b tel que $b \geqslant a$, $b \neq a$ et que $b \geqslant c \geqslant a$ entraîne soit $c = b$, soit $c = a$.

Supposons qu'un certain nombre a n'ait pas de successeur. Cela veut dire que, pour n'importe quel $a_n \geqslant a$ différent de a, il y a un a_{n+1} différent tant de a_n que de a et tel que $a_n \geqslant a_{n+1} \geqslant a$. Prenons maintenant un nombre $a_1 \geqslant a$ quelconque différent de a (ce qui, en vertu de 2°, est possible) et, en le prenant pour point de départ, construisons une suite infinie de nombres distincts

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant a_{n+1} \geqslant \ldots \geqslant a.$$

L'existence de cette suite contredit 4°. En conséquence, le successeur existe. Son unicité s'établit au moyen de la dichotomie de façon dont on l'a fait dans a) et b).

9. La transitivité (3°), le fait pour l'ensemble de nombres naturels d'être illimité (5°), la propriété 4° et l'existence d'un antécédent (6°) restent valables. La dichotomie est remplacée par la *trichotomie* (ou bien $a > b$, ou bien $b > a$, ou bien $a = b$).

La propriété 1° (réflexivité) cesse d'être vraie, car $a > a$ est toujours inexact.

Quant à la propriété 2°, elle reste formellement valable.

En effet, à strictement parler, dans notre cas elle s'énonce ainsi : pour tous nombres naturels a et b, $a > b$ et $b > a$ entraînent $a = b$.

Supposons que cette proposition soit fausse. Il y aura alors des nombres naturels a et b tels qu'on aurait en même temps $a > b$, $b > a$ et $a \neq b$, ce qui est impossible. La contradiction obtenue prouve la justesse de notre proposition.

10. Comme nous l'avons déjà établi, notre ensemble possède un élément minimal. Désignons-le par a_0. Il découle des résultats du problème 8 que chaque élément a le successeur. Désignons le successeur de a_0 par a_1, celui de a_1 par a_2, etc. On obtient ainsi la suite

$$a_0, a_1, a_2, \ldots, \tag{23}$$

dans laquelle $a_{n+1} \succcurlyeq a_n$ quel que soit n. En vertu de la réflexivité et de la transitivité de la relation $\succcurlyeq$, il en résulte que $a_i \succcurlyeq a_j$ si, et seulement si, $i \geqslant j$. Il nous reste à montrer que la suite (23) comprend tous les objets considérés ; on y parvient par un raisonnement par récurrence assez subtil.

Supposons que b_0 ne fasse pas partie de la suite (23). Nous considérerons l'obtention de b_0 comme le premier pas de notre raisonnement par récurrence. Supposons qu'au bout de n pas nous parvenions à un certain élément b_{n-1}.

Si $b_{n-1} = a_0$, notre processus est achevé ; si, par contre, $b_{n-1} \neq a_0$, l'élément b_{n-1} a l'antécédent que nous prendrons pour b_n. En conséquence, nous obtenons une suite d'éléments distincts

$$b_0 \succcurlyeq b_1 \succcurlyeq b_2 \succcurlyeq \ldots \succcurlyeq b_n \succcurlyeq \ldots$$

En vertu de 4°, cette suite doit avoir un dernier terme. Mais selon le principe même de la construction de cette suite, son dernier terme ne peut être que a_0. Soit, pour fixer les idées, $b_n = a_0$.

On vérifie aisément que si un certain nombre a est l'antécédent de b, b est le suivant de a. Donc $b_{n-1} = a_1$, $b_{n-2} = a_2$, . . ., $b_0 = a_n$.

Cette dernière égalité signifie que b_0 fait partie de la suite (23), mais cela contredit notre supposition. En conséquence, la suite (23) renferme tous les objets considérés.

11. Soit a un nombre quelconque. Appelons *chaîne d'éléments précédant* a_0 toute suite de nombres distincts $a_0 = a, a_1, a_2, \ldots, a_n$ pour lesquels

$$a_0 \succ a_1 \succ a_2 \succ \ldots \succ a_n, \tag{24}$$

où a_n est minimal au sens de la relation d'ordre $\succ$. Le nombre n est la *longueur* de cette chaîne.

Montrons d'abord que, dans les conditions que nous avons imposées à la relation d'ordre $\succ$, chaque nombre concret ne peut avoir une chaîne d'éléments précédents arbitrairement longue.

En effet, soient a un certain nombre et $b_1, b_2, \ldots, b_k$ ses prédécesseurs.

Si a_1 n'est pas le prédécesseur de a_0, on peut, en vertu de 9°, insérer dans la chaîne (24) un nombre qui soit le prédécesseur de a. Par conséquent, s'il existe des chaînes aussi longues que l'on veut d'éléments précédant a, il y en a dont le premier terme soit le prédécesseur de a. Bornons-nous à ne considérer que de telles chaînes.

Chaque chaîne d'éléments précédant a est exactement d'une unité plus longue qu'une certaine chaîne d'éléments précédents de l'un de ses prédécesseurs. Si chacun de ceux-ci avait des chaînes d'éléments précédents bornées, le nombre a lui-même ne pourrait avoir des chaînes d'éléments précédents aussi longues que l'on veut.

Donc, sous notre supposition, pour l'un au moins des prédécesseurs de a_0 des chaînes d'éléments précédents sont aussi longues que l'on veut. Désignons ce prédécesseur par a_1 et répétons tous les raisonnements ci-dessus. Cela nous donnera un certain nombre a_2, antécédent de a_1, ayant des chaînes d'éléments précédents aussi longues que l'on veut. En réitérant ce processus, nous arrivons à la suite

$$a_0 \succ a_1 \succ a_2 \succ \ldots$$

qui, en vertu de 4°, doit se terminer tôt ou tard. Cela veut dire que la suite aura un terme tel qu'on ne pourra plus lui appliquer nos raisonnements. Or, nous avons établi que nos raisonnements s'appliquent à chacun des termes successifs de la suite. La contradiction ainsi obtenue prouve que pour aucun nombre on ne peut former des chaînes d'éléments précédents aussi longues que l'on veut.

En conséquence, parmi les chaînes d'éléments précédant tout nombre a on peut choisir la chaîne maximale. Désignons sa longueur par $n(a)$. Si b est le prédécesseur de a, on a évidemment $n(b) = n(a) - 1$ et, pour tous les a minimaux, $n(a) = 0$.

Soit, pour finir, $A(a)$ une proposition dépendant de a. Désignons par $B(n)$ la proposition selon laquelle $A(a)$ est juste pour tous les nombres a pour lesquels $n(a) = n$. Dans ce cas, comme on le voit aisément, l'énoncé du nouveau mode de raisonnement par récurrence pour $A(a)$ coïncide avec l'énoncé sous forme ancienne pour $B(n)$.

12. a) Quels que soient les nombres pairs a et b, il existe des nombres pairs q et r tels que

$$a = bq + \quad (0 \leqslant r < 2b). \tag{25}$$

De tels nombres q et r sont uniques.

● DÉMONSTRATION. D'après le théorème 7, il existe des nombres q_0 et r_0 tels que

$$a = bq_0 + r_0 \, (0 \leqslant r_0 \leqslant q_0).$$

En vertu du théorème 6, r_0 doit être pair. Si q_0 est également pair, on peut poser $q = q_0$ et $r = r_0$. Si, par contre, q_0 est impair, on a $q = q_0 - 1$ (un tel q est évidemment pair) et $r = r_0 + b$. Dans les deux cas on obtient la relation (25).

Supposons qu'en plus de (25) on ait encore une autre représentation:

$$a = bq' + r' \, (0 \leqslant r' < 2b),$$

où les nombres q et r sont pairs. On a alors

$$b(q' - q) = r - r'.$$

Comme

$$0 \leqslant |r - r'| < 2b,$$

on doit avoir $|q' - q| < 2$. Mais $q' - q$ est un nombre pair. Donc, $q' - q = 0$, d'où l'on tire aisément le résultat cherché.

13. Soit p le plus petit diviseur premier du nombre a. Il s'ensuit que $a = pb$. Tout diviseur premier q du nombre b est en même temps diviseur de a. Aussi $q \geqslant p$, donc $b \geqslant p$, de sorte que $a \geqslant p^2$ et, enfin, $p \leqslant \sqrt{a}$.

14. Condition nécessaire. Soit $a \,\vdots\, b$. Il découle du théorème 13 que chaque diviseur premier de b est aussi un diviseur premier de a. De la sorte, b se présente sous la forme

$$p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \tag{26}$$

où $0 \leqslant \beta_1$, $0 \leqslant \beta_2$, ..., $0 \leqslant \beta_k$. Supposons que $\beta_1 > \alpha_1$. Comme

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}} = \frac{p_2^{\alpha_2} \ldots p_k^{\alpha_k}}{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \ldots p_k^{\beta_k}}$$

est un nombre entier, le numérateur de la dernière fraction doit être divisible par le dénominateur et, a fortiori, par le nombre $p_1^{\beta_1-\alpha_1}$. Mais alors, d'après le théorème 13, l'un au moins des nombres $p_2, \ldots, p_k$ doit être divisible par p_1, ce qui est impossible. Donc, $\beta_1 \leqslant \alpha_1$. Comme la numérotation des diviseurs premiers de a n'a pas d'importance, nous avons démontré par là même que $\beta_2 \leqslant \alpha_2, \ldots$ $\ldots, \beta_k \leqslant \alpha_k$. La nécessité est démontrée.

Pour démontrer la *suffisance*, remarquons que si b a la forme indiquée, alors

$$a = b p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \ldots p_k^{\alpha_k - \beta_k}.$$

15. Comme nous l'avons déjà établi, chaque diviseur du nombre a à décomposition canonique $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ doit avoir la forme (26), où β_1 prend $\alpha_1 + 1$ valeurs: 0, 1, 2, ..., α_1; β_2 prend $\alpha_2 + 1$ valeurs, etc. Comme toutes les combinaisons de ces valeurs sont possibles et nous fournissent tous les diviseurs de a, chaque diviseur étant obtenu une seule fois (si un diviseur quelconque se répétait, cela impliquerait que le nombre a a plusieurs décompositions canoniques), le nombre de diviseurs de a est de

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1).$$

16. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la décomposition canonique de a. On peut évidemment poser $p_1 = 2$, $\alpha_1 \geqslant 2$ et $p_2 = 3$, $\alpha_2 \geqslant 1$. Ensuite, on a:

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) = 14,$$

d'où $k = 2$, $\alpha_1 + 1 = 7$ et $\alpha_2 + 1 = 2$. De la sorte, $a = 2^6 \cdot 3 = 192$.

17. On a:

$$\tau(a^2) = \tau(p_1^{2\alpha_1} p_2^{2\alpha_2}) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 81,$$

de sorte que $(2\alpha_1 + 1)(2\alpha_2 + 1)$ est la décomposition du nombre 81 en deux facteurs. Comme la numérotation des diviseurs premiers de a dépend de nous, nous nous bornons à examiner les possibilités suivantes:

$$2\alpha_1 + 1 = 1, \quad 2\alpha_2 + 1 = 81,$$
$$2\alpha_1 + 1 = 3, \quad 2\alpha_2 + 1 = 27,$$
$$2\alpha_1 + 1 = 9, \quad 2\alpha_2 + 1 = 9.$$

Dans le premier cas, $\alpha_1 = 0$, ce qui est contraire à la positivité supposée du nombre α_1. Les autres cas nous donnent

$$\alpha_1 = 1, \quad \alpha_2 = 13,$$
$$\alpha_1 = 4, \quad \alpha_2 = 4.$$

Donc, ou bien

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_2}) = \tau(p_1^3 p_2^{39}) = (3+1)(39+1) = 160,$$

ou bien

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_2}) = \tau(p_1^{12} p_2^{12}) = 13 \cdot 13 = 169.$$

18. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la décomposition canonique du nombre a. Par hypothèse, on a

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = 2(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1),$$

ou encore

$$\frac{p_1^{\alpha_1}}{\alpha_1 + 1} \frac{p_2^{\alpha_2}}{\alpha_2 + 1} \cdots \frac{p_k^{\alpha_k}}{\alpha_k + 1} = 2. \qquad (27)$$

Notons que

$$\frac{2^1}{1+1} = 1 < \frac{2^2}{2+1} < \frac{2^3}{3+1} = 2 < \frac{2^\alpha}{\alpha+1} \quad (\alpha \geqslant 4),$$

$$1 < \frac{3^1}{1+1} < 2 < \frac{3^\alpha}{\alpha+1} \quad (\alpha \geqslant 2),$$

$$2 < \frac{p^\alpha}{\alpha+1} \quad (p \geqslant 5, \ \alpha \geqslant 1).$$

Aussi toute fraction du premier membre de (27) est au moins égale à l'unité et, en conséquence, aucune fraction ne peut être supérieure à 2. Donc, le premier membre de (27) ne peut contenir que les fractions de l'ensemble suivant:

$$\frac{2^1}{1+1}, \quad \frac{2^2}{2+1}, \quad \frac{2^3}{3+1}, \quad \frac{3^1}{1+1},$$

dont le produit est 2. Mais la chose n'est possible que dans deux cas: quand le premier membre de (27) ne contient que la fraction $\frac{2^3}{3+1}$ ou les deux fractions $\frac{2^2}{2+1}$ et $\frac{3^1}{1+1}$. A ces deux cas correspondent les deux réponses, à savoir: 8 et 12.

19. Les théorèmes analogues aux théorèmes 11-14 ne sont pas valables pour la divisibilité paire.

En effet, les nombres 30 et 42 sont pairement premiers. Ils admettent le plus petit commun multiple pair 420 et leur produit est 1260.

Ensuite, $60 = 6 \cdot 10$ est divisible de façon paire par le nombre pairement premier 30; les nombres 6 et 30 sont pairement premiers entre eux, tandis que le nombre 10 n'est pas divisible de façon paire par 30.

Finalement, $60 = 6 \cdot 10 = 30 \cdot 2$ sont des décompositions différentes du nombre 60 en facteurs pairement premiers.

20. Soit $p_1, p_2, \ldots, p_k$ l'ensemble de tous les nombres premiers faisant partie de l'une des décompositions canoniques de a et de b au moins. Posons

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}.$$

(Si a n'est pas divisible par p_i, on a $\alpha_i = 0$; si b n'est pas divisible par p_i, alors $\beta_i = 0$.) Soit γ_i le plus grand des nombres α_i et β_i pour $i = 1, 2, \ldots, k$ et δ_i le plus petit de ces nombres.

Dans ce cas, en vertu de ce que l'on a établi en résolvant le problème 13, le plus grand commun diviseur de a et b est $p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}$ et leur plus petit commun multiple $p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$.

21. a) Quand on les divise par 8, 116 et 4 donnent le même reste, ainsi que 17 et 1. Donc, il en est de même de A et de $5^{21} = (5^2)^{10} \cdot 5$. De son côté, la division de $5^2 = 25$ et de 1 par 8 donne les restes égaux. Par conséquent, le reste de la division de A par 8 est 5.

b) Quand on les divise par 17, 14 et -3 donnent le même reste. C'est pourquoi il en est de même de A et de

$(-3)^{256} = 3^{256} = (3^3)^{85}\cdot 3$. Mais on peut remplacer 3^3 par $10: 10^{85}\cdot 3 = (10^2)^{42}\cdot 30$. Ensuite, quand on les divise par 17, 10^2 et -2, d'une part, et 2^4 et -1, d'autre part, donnent les restes égaux. Donc, A donne le même reste que $(-2)^{42}\times \times 30 = 2^{42}\cdot 30 = (2^4)^{10}\cdot 4\cdot 30 = (-1)^{10}\cdot 4\cdot 30 = 120$. Le reste de la division de ce dernier nombre par 17 est 1.

22. a) Soit n_1 le reste de la division de n par 6. Dans ce cas, n_1 peut prendre les valeurs 0, 1, 2, 3, 4 et 5, et la division de $n_1^3 + 11n_2$ et de $n^3 + 11n$ par 6 donne le même reste. Il nous faut donc essayer la divisibilité par 6 des nombres 0, 12, 30, 60, 108 et 180. Or, chacun de ces nombres est divisible par 6.

b) Pour $n \geqslant 2$, on a (en utilisant la formule du binôme) :

$$4^n + 15n - 1 = (3+1)^n + 15n - 1 =$$

$$= 3^n + 3^{n-1}C_n^1 + \ldots + 3^2C_n^{n-2} + 3C_n^{n-1} + 1 + 15n - 1 =$$

$$= 9\,(3^{n-2} + 3^{n-3}C_n^1 + \ldots + C_n^{n-2}) + 18n,$$

et les deux termes sont évidemment divisibles par 9.

Pour $n = 1$, notre expression vaut $4^1 + 15\cdot 1 - 1 = 18$.

c) La démonstration se fait par récurrence.

Pour $n = 0$

$$10^{3^0} - 1 = 10^1 - 1 = 9 \quad \text{et} \quad 3^{0+2} = 9.$$

Supposons maintenant que la divisibilité

$$10^{3^n} - 1 \,\vdots\, 3^{n+2}$$

soit possible. Dans ce cas

$$10^{3^{n+1}} - 1 = (10^{3^n})^3 - 1^3 = (10^{3^n} - 1)\,(10^{2\cdot 3^n} + 10^{3^n} + 1).$$

Le premier facteur du deuxième membre est divisible par 3^{n+2} selon l'hypothèse de récurrence. Dans le deuxième facteur, on peut remplacer les dizaines par des unités qui, quand on les divise par 3, donnent le même reste ; le nombre 3 obtenu montre que le deuxième facteur est divi-

sible par 3. Par conséquent, le produit tout entier est divisible par $3^{n+3} = 3^{3(n+1)+2}$, C.Q.F.D.

d) Il est évident que, quand on les divise par $a^2 - a + 1$, a^2 et $a - 1$ donnent le même reste. Donc, il en est de même de $a^{2n+1} + (a - 1)^{n+2}$ et

$$a^{2n+1} + (a^2)^{n+2} = a^{2n+1} + a^{2n+4} = a^{2n+1}(1 + a^3) = \\ = a^{2n+1}(1 + a)(1 - a + a^2),$$

C.Q.F.D.

23. Soit $\sim$ une relation d'équivalence sur un ensemble de nombres. Prenons un nombre a quelconque et considérons tous les nombres équivalents à a. En vertu de la transitivité de la relation $\sim$, ils sont tous équivalents entre eux. Désignons par K la classe formée par tous ces nombres.

Considérons maintenant un nombre b quelconque non contenu dans K. Si l'on avait $b \sim c$, où c est un certain nombre de K, on aurait également $b \sim a$, ce qui est impossible vu le choix de b. Donc, aucun des nombres non appartenant à K n'est équivalent à aucun des nombres de K. Par conséquent, K est une classe d'équivalence contenant a.

Comme nous avons choisi le nombre a d'une façon absolument arbitraire, les raisonnements que nous venons de tenir montrent que tout nombre appartient à une certaine classe d'équivalence. C.Q.F.D.

24. Il est évident que parmi les nombres $0, 1, \ldots, m$ il s'en trouvera deux qui appartiennent à la même classe. Supposons que ces nombres soient k et l: $k \sim l$. D'une façon générale, il peut y avoir plusieurs couples de ce genre dans une même classe. Choisissons celui d'entre eux pour lequel la grandeur $|k - l|$ est maximale. Etant donné que $-l \sim -l$, on a par hypothèse

$$k - l \sim l - l = 0.$$

Ensuite, on constate que, pour tout entier n, on a de même

$$n(k - l) \sim 0.$$

Finalement, pour n'importe quel r,

$$n(k - l) + r \sim r,$$

c.-à-d. que $a \equiv b \pmod{k - l}$ entraîne $a \sim b$. De la sorte, les classes résiduelles modulo m sont entièrement contenues dans les classes de la relation $\sim$.

Pour qu'il y ait m classes d'équivalence $\sim$, il faut que chaque classe d'équivalence $\sim$ contienne au plus une classe résiduelle et que $k - l = m$.

25. a) Les deux membres de la congruence et le module sont divisibles par le même nombre (évidemment différent de 0).

En effet,

$$ad \equiv bd \pmod{md}$$

signifie que

$$ad - bd = (a - b)d \vdots md,$$

c.-à-d. que $a - b \vdots m$, d'où $a \equiv b \pmod{m}$.

b) Les deux membres de la congruence sont divisibles par un nombre premier avec le module.

En effet, en vertu du théorème 12, si d et m sont premiers entre eux, il découle de

$$ad \equiv bd \pmod{m},$$

c.-à-d. de $(a - b)d \vdots m$, que $a - b \vdots m$, C.Q.F.D.[1]

26. Supposons que $1 \leqslant k < l \leqslant p - 1$, $ka \equiv la \pmod{p}$. Cela signifie que $(l - k)\, a \vdots p$. Etant donné que a n'est pas divisible par p, on devrait avoir $l - k \vdots p$. Mais cela est impossible, car $0 < l - k < p$.

27. Nécessité. Soit p un nombre premier. Posons $0 < q < p$. Parmi les nombres $q, 2q, \ldots, (p - 1)\, q$, il s'en trouvera exactement un qui, divisé par p, donnera 1 pour reste. Soit $\bar{q}q$ ce nombre:

$$\bar{q}q \equiv 1 \pmod{p}. \qquad (28)$$

Parallèlement, parmi les nombres $\bar{q}, 2\bar{q}, \ldots, (p - 1)\, \bar{q}$, il ne peut y en avoir qu'un qui, divisé par p, donne 1 pour reste. Comme nous l'avons déjà établi, il s'agit du nombre $q\bar{q}$.

Voyons dans quel cas $q = \bar{q}$. Dans tous les cas de ce genre, la congruence (28) se récrit comme suit:

$$q^2 \equiv 1 \pmod{p},$$

ou, ce qui revient au même,

$$q^2 - 1 \equiv 0 \pmod{p}.$$

Cela signifie que

$$q^2 - 1 = (q + 1)(q - 1) \vdots p.$$

Etant donné que le nombre p est premier, d'après le théorème 13, on doit avoir soit $q+1 \vdots p$, soit $q-1 \vdots p$. Comme le nombre q est compris entre 0 et p, le premier cas n'est possible que pour $q = p - 1$ et le deuxième pour $q = 1$.

En conséquence, on peut former avec les nombres restants 2, ..., $p - 2$ des couples tels que, quand on le divise par p, le produit des nombres de chaque couple admet 1 pour reste. Ecrivons les congruences de la forme (28) pour tous les couples de ce type, ajoutons la con-

gruence

$$p-1 \equiv p-1 \pmod p$$

et multiplions terme à terme tous les $\frac{p+1}{2}$ congruences obtenues.

Le premier membre comprendra alors le produit de tous les nombres de 2 à $p-1$ (ce dernier figurera deux fois), et le deuxième membre sera l'unité:

$$2\cdot 3 \ldots (p-1)(p-1) \equiv 1 \pmod p,$$

c'est-à-dire

$$2\cdot 3 \ldots (p-1) \equiv p-1 \pmod p,$$

ou

$$1\cdot 2\cdot 3 \ldots (p-1)+1 \equiv 0 \pmod p.$$

Cette dernière relation signifie que

$$1\cdot 2 \ldots (p-1)+1 \,\vdots\, p,$$

C.Q.F.D.

Suffisance. Si le nombre p n'est pas premier, il peut être décomposé en un produit de deux facteurs plus petits: $p = p_1p_2$.

Si $p_1 \neq p_2$, p_1 et p_2 sont des facteurs du produit $1\cdot 2 \ldots (p-1)$ qui est de ce fait divisible par p_1p_2, c.-à-d. par p. Soit maintenant $p_1 = p_2 = q$. Dans ce cas, $p = q^2$ (c.-à-d. que p est le carré d'un nombre premier). Si $q > 2$, on a $p > 2q$, et le produit $1\cdot 2 \ldots (p-1)$ a pour facteurs q et $2q$, de sorte que dans ce cas il est divisible par q^2, c.-à-d. par p. Dans les deux cas, $1\cdot 2 \ldots (p-1)+1$ ne peut être divisible par p. Enfin, si $p = 4$, alors $1\cdot 2\cdot 3 - 1 = 5$ et n'est pas divisible par 4.

28. THÉORÈME. *Soit* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *la décomposition canonique de* m. *Dans ce cas pour que les nombres* A *et* B *soient congrus modulo* m, *il faut et il suffit qu'ils soient congrus modulo* $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots$ *...,* $p_k^{\alpha_k}$.

● DÉMONSTRATION. *Condition nécessaire.* La congruence modulo m des nombres A et B signifie que $A - B \,\vdots\, m$. A fortiori $A - B \,\vdots\, p_i^{\alpha_i}$ $(i = 1, \ldots, k)$, et les nombres A et B divisés par tous les $p_i^{\alpha_i}$ admettent le même reste.

Condition suffisante. Supposons que, si on les divise par chaque $p_i^{\alpha_i}$, les nombres A et B donnent le même reste. Désignons par r_i le reste de la division de A et B par $p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$. Cela si-

gnifie que

$$A \equiv r_i \pmod{p_i^{\alpha_i}}. \qquad (29)$$

Supposons ensuite que

$$\frac{m}{p_i^{\alpha_i}} = m_i, \qquad i = 1, \ldots, k,$$

et multiplions tous les termes de (29) par m_i:

$$A m_i \equiv m_i r_i \pmod{m}.$$

En ajoutant terme à terme toutes ces congruences, on obtient

$$A (m_1 + m_2 + \ldots + m_k) \equiv m_1 r_1 + m_2 r_2 + \ldots + m_k r_k \pmod{m}. \qquad (30)$$

Etant donnée la congruence modulo $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ de A et B on a également

$$B (m_1 + m_2 + \ldots + m_k) \equiv m_1 r_1 + m_2 r_2 + \ldots + m_k r_k \pmod{m}. \qquad (31)$$

En retranchant terme à terme (31) de (30), on a

$$(A - B)(m_1 + m_2 + \ldots + m_k) \equiv 0 \pmod{m},$$

c'est-à-dire $(A - B)(m_1 + m_2 + \ldots + m_k) \vdots m$.

Mais la somme $m_1 + m_2 + \ldots + m_k$ et le nombre m sont premiers entre eux. En effet, si cette somme et m avaient un diviseur premier commun p, celui-ci ferait partie de la décomposition canonique de m, c.-à-d. qu'il aurait la forme p_i. Mais dans ce cas il serait diviseur tant de la somme entière que de chacun de ses termes sauf un, à savoir m_i, ce qui est impossible.

Nous pouvons maintenant appliquer le théorème 12, qui nous permet d'établir que $A - B \vdots m$, c.-à-d. que les nombres A et B divisés par m donnent le même reste.

29. a) Ecrivons le système d'égalités qui décrivent les divisions euclidiennes appliquées aux nombres a et b:

$$\left.\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1 q_1 + r_2, \\ r_1 &= r_2 q_2 + r_3, \\ &\ldots\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\ r_{n-1} &= r_n q_n. \end{aligned}\right\} \qquad (32)$$

On a $r_{n-1} \vdots r_n$. Compte tenu de $r_{n-2} = r_{n-1} q_{n-1} + r_n$, on en déduit que $r_{n-2} \vdots r_n$. En montant dans le système d'égalités (32), on obtient enfin $a \vdots r_n$ et $b \vdots r_n$. Donc, r_n est le diviseur commun à a et b.

Soit d un diviseur commun quelconque de a et b. Compte tenu de $a = bq_0 + r_1$, on en déduit que $r_1 \vdots d$. En descendant dans le système d'égalités (32), on a successivement $r_2 \vdots d$, $r_3 \vdots d, \ldots, r_n \vdots d$. Donc, r_n est divisible par tout diviseur commun à a et b, c'est donc le plus grand commun diviseur de ces nombres.

b) La démonstration se fait par récurrence. En posant $A_0 = 0$, $B_0 = 1$, $A_1 = 1$, $B_1 = -q_0$, on a $r_0 = b = aA_0 + bB_0$ et $r_1 = aA_1 + bB_1$. Soit maintenant

$$r_{k-1} = A_{k-1}a + B_{k-1}b,$$
$$r_k = A_k a + B_k b,$$

mais alors

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = (A_{k-1} - q_{k+1}A_k)\,a + (B_{k-1} - q_{k+1}B_k)\,b,$$

et il nous reste à poser

$$A_{k-1} - q_{k+1}A_k = A_{k+1},$$
$$B_{k-1} - q_{k+1}B_k = B_{k+1}.$$

A_n et B_n sont donc les nombres A et B cherchés.

30. Si b et c sont premiers entre eux, on peut, d'après ce qui précède, trouver des nombres entiers B et C tels que

$$bB + cC = 1,$$

ou, en multipliant par a,

$$abB + acC = a;$$

$ab \vdots c$ par hypothèse; $ac \vdots c$ est évident; donc $a \vdots c$.

31. Bornons-nous à considérer le caractère de congruence modulo 8.

Soit A un nombre naturel quelconque représenté sous la forme $1000\,a + b$, où $0 \leqslant b < 1000$ (c.-à-d. que b est le nombre de trois chiffres par lequel se termine A) et

$$f(A) = \begin{cases} b \text{ si } A \geqslant 1000, \\ \text{reste de la division de } A \text{ par 8 si } 8 \leqslant A < 1000, \\ \text{n'est pas définie si } A < 8. \end{cases}$$

32. Ceux dont les décompositions canoniques ont la forme $2^{\alpha} \cdot 5^{\beta}$.

33. Les conditions a) et b) sont remplies automatiquement. Etant donné que 10 est congru à 1 modulo 3, il doit

en être de même des nombres A et $f(A)$. Enfin, on établit par un simple calcul que $f(A) < A$ pour $A \geqslant 3$.

34. a) $f(858\,773) = 38$; $f(38) = 11$; $f(11) = 2$.

b) $f(\mathrm{A}) = 4444 \cdot 4 = 17\,776$; $f(17\,776) = 28$; $f(28) = 10$; $f(10) = 1$.

35. Le caractère de congruence modulo 9 est analogue au caractère de congruence modulo 3.

Pour obtenir le caractère de congruence modulo 11, représentons le nombre A sous la forme

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \ldots + 10^2a_1 + a_0,$$

où $0 \leqslant a_i < 100$. Il est évident qu'une telle représentation correspond à la partition du nombre en tranches binaires (de droite à gauche). Soit

$$f(A) = \begin{cases} a_0 + a_1 + \ldots + a_n \text{ si } A \geqslant 100, \\ \text{reste de la division de } A \text{ par } 11 \text{ si } 11 \leqslant A < 100, \\ \text{n'est pas définie si } A < 11. \end{cases}$$

Il nous reste à indiquer que A est congru à $f(A)$ modulo 11 et que $f(A) < A$.

Un autre caractère de congruence modulo 11 s'obtient sur la base de la représentation du nombre A sous la forme

$$A = 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10a_1 + a_0$$

et en s'appuyant sur le fait que 10 est congru à -1 modulo 11 et 100 à 1. Les nombres A et $a_0 - a_1 + a_2 - a_3 + \ldots$ $\ldots \pm a_n$ donnent donc des restes égaux, et l'énoncé du caractère correspondant ne présente aucune difficulté.

Enfin, on peut, en partageant le nombre A en tranches ternaires, le représenter sous la forme

$$10^{3n}a_n + 10^{3n-3}a_{n-1} + \ldots + 10^3a_1 + a_0$$

$(0 \leqslant a_i < 1000)$. Dans ce cas, A est congru à la somme $a_0 + a_1 + \ldots + a_n$ modulo 37 et à la somme alternée $a_0 - a_1 + a_2 - \ldots \pm a_n$ modulo 7, 11 et 13.

36. Si les nombres a et b sont congrus par rapport à m $a - b : m$. Donc, en vertu du théorème 6, les nombres a et b sont simultanément divisibles ou non par m. 4 et 5 sont équidivisibles par 3, mais ne sont pas congrus modulo 3.

37. Supposons que l'équidivisibilité par m entraîne la congruence par rapport au module m. Cela signifie que tous les nombres non divisibles par m sont congrus modulo m. Donc, le reste doit être 1, ce qui fait que $m = 2$.

38. La relation d'équidivisibilité par m est évidemment réflexive (tout nombre est équidivisible par m avec lui-même), symétrique (si a et b sont équidivisibles, b et a le sont aussi) et transitive (si a et b sont équidivisibles et que b et c le soient aussi, il en est de même de a et c).

Par conséquent, il s'agit d'une relation d'équivalence, l'une des classes comprenant tous les nombres divisibles par m et l'autre tous les nombres qui ne le sont pas.

39. On vérifie aisément que, pour $m > 2$, l'équidivisibilité des sommes ne découle pas de l'équidivisibilité des termes.

Pour que l'équidivisibilité des produits découle de celle de leurs facteurs, il faut et il suffit que le nombre m soit premier.

En effet, si l'un des produits est divisible par un nombre premier p, en vertu du théorème 13, l'un au moins des facteurs de ce produit doit l'être également. Mais alors le facteur d'un autre produit, qui est équidivisible avec ce facteur, est lui aussi divisible par p, et il en est de même du produit tout entier. Si, par contre, l'un des produits n'est pas divisible par p, l'autre ne peut l'être non plus (sinon, en vertu de ce que l'on vient d'établir, le premier produit serait lui aussi divisible par p).

Par contre, si p est composé, les produits de facteurs équidivisibles peuvent ne plus être équidivisibles. Il suffit de poser $p = p_1p_2$ ($p_1 \neq 1$, $p_2 \neq 1$), auquel cas les nombres 1 et p_1, de même que 1 et p_2, sont équidivisibles par p, tandis que leur produit ne l'est évidemment pas.

40. Corollaire du problème 36a).

41. C'est évident pour les conditions a) et b).

Si $a - b \geqslant 0$, il est évident que $f(A) < A$. Si, par contre, $a - 2b < 0$, il se peut que cette inégalité soit fausse. Le module $|a - 2b|$ atteint sa plus grande valeur pour $a = 0$ et $b = 9$, elle est égale donc à 18. En conséquence, pour $A \geqslant 19$, on doit avoir $f(A) < A$. La justesse de cette inégalité pour des valeurs inférieures est assurée par la détermination de la fonction f.

Enfin, $10a + b$ est équidivisible par 7 avec $50a + 5b$ (car 5 et 7 sont premiers entre eux), donc avec $50a + 5b - 7(7a + b) = a - 2b$.

42. 15 divisé par 7 donne 1 pour reste, tandis que $1-2\cdot 5=-9$ et le reste de la division de 9 par 7 est 5.

43. Condition c). $f(A) < A$ signifie que $a + 4b < 10a + b$, c'est-à-dire que $3b < 9a$. Aussi, pour $a \geqslant 4$, la condition nécessaire est-elle remplie.

Condition d). Il est évident que, quand on les divise par 13, $10a + b$ et $40a + 4b$ sont équidivisibles et que ce dernier nombre est congru à $a + 4b$.

44. Le caractère de divisibilité n'est plus efficace car $f(39) = 39$.

45. Supposons qu'il nous faille établir le caractère de divisibilité par un certain m. Essayons de trouver un s premier avec m qui soit petit et tel que $10s + 1 \vdots m$ (il en a été ainsi pour $m = 7$; s s'est alors avéré égal à 3) ou bien que $10s - 1 \vdots m$ (ainsi, pour $m = 13$, on a $s = 4$).

Dans le premier cas, $A = 10a + b$ et

$$10as + bs = (10s + 1)\,a - a + bs,$$

c.-à-d. $a - bs$, sont équidivisibles par m; dans le deuxième cas, il s'agit de l'équidivisibilité par m de $A = 10a + b$ et de

$$(10s - 1)\,a + a + bs,$$

c'est-à-dire $a + bs$.

En conséquence,

$10a + b$ et	$a - 5b$	sont	équidivisibles par	17,
»	$a + 2b$	»	»	19,
»	$a + 7b$	»	»	23,
»	$a - 3b$	»	»	29,
»	$a + 3b$	»	»	31.

Nous laissons au lecteur le soin d'achever les énoncés rigoureux de ces caractères de divisibilité.

46. a) Etant donné que 100 est congru à 2 modulo 49, tout nombre de la forme

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \ldots + 10^2a_1 + a_0 \quad (0 \leqslant a_i < 100)$$

est congru à

$$2^n a_n + 2^{n-1}a_{n-1} + \ldots + 2a_1 + a_0$$

modulo 49.

b) $10a + b$ et $a + 5b$ sont équidivisibles par 49.

47. Les conditions a) et b) sont remplies automatiquement. Les conditions c) et d) sont satisfaites parce que le passage de A à $F(A)$ se ramène au remplacement de certains nombres par les restes de leur division par A (qui sont inférieurs à ces nombres mêmes et donnent les mêmes restes).

48. a) $r_2 = r_3 = \ldots = r_n = 0$, c.-à-d. $r_k = 0$ $(k \geqslant 2)$;

b) $r_3 = r_4 = \ldots = r_n = 0$, c.-à-d. $r_k = 0$ $(k \geqslant 3)$;

c) $r_1 = r_2 = \ldots = r_n = 1$, c.-à-d. $r_k = 1$;

d) $r_1 = r_3 = \ldots = r_{2l-1} = -1$, $r_2 = r_4 = \ldots$ $\ldots = r_{2l} = 1$, c.-à-d. $r_k = (-1)^k$;

e) $r_{6l+1} = 3$, $r_{6l+2} = 2$, $r_{6l+3} = 6$, $r_{6l+4} = 4$, $r_{6l+5} = 5$, $r_{6l} = 1$.

49. Nous en laissons le soin au lecteur.

50. Ni $2^4 - 2$ ni $2^3 - 1$ ne sont divisibles par 4.

51. Si $a \,\vdots\, p$, alors $a^p \,\vdots\, p$, et le théorème est démontré. Si, par contre, a n'est pas divisible par p, a et p sont premiers entre eux, et nous pouvons simplifier la congruence

de l'énoncé du théorème:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Pour démontrer cette dernière relation, divisons avec reste chacun des nombres de la forme ta ($t = 1, 2, \ldots$ $\ldots, p-1$) par p:

$$ta = q_t p + r_t,$$

ce qu'on peut récrire comme suit:

$$\left.\begin{aligned} a &\equiv r_1 \pmod{p}, \\ 2a &\equiv r_2 \pmod{p}, \\ &\ldots\ldots\ldots\ldots \\ (p-1)\,a &\equiv r_{p-1} \pmod{p}. \end{aligned}\right\} \qquad (33)$$

Il découle du résultat du problème 26 que chacun des nombres $1, 2, \ldots, p-1$ figure une fois parmi les nombres r. En multipliant toutes les congruences (33), on obtient

$$1 \cdot 2 \ldots (p-1)\, a^{p-1} \equiv 1 \cdot 2 \ldots (p-1) \pmod{p}.$$

Il nous reste à diviser cette relation par $1 \cdot 2 \ldots (p-1)$.

52. $\varphi(12) = \varphi(2^2 \cdot 3) = 2^{2-1}(3-1) = 2 \cdot 2 = 4$,

$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^{3-1}(3-1)(5-1) =$ $= 4 \cdot 2 \cdot 4 = 32$,

$\varphi(1000) = \varphi(2^3 5^3) = 2^{3-1} 5^{3-1}(5-1) = 4 \cdot 25 \cdot 4 =$ $= 400$.

53. Cherchons m sous la forme $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, auquel cas

$$\text{a)}\ p_1^{\alpha_1-1}(p_1-1)\, p_2^{\alpha_2-1}(p_2-1) \ldots p_k^{\alpha_k-1}(p_k-1) = 10.$$

Le produit du premier membre doit être divisible par 5, donc, ou bien l'un des nombres $p_1, p_2, \ldots, p_k$ est 5 (supposons, pour fixer les idées, que $p_1 = 5$), ou bien l'une des différences $p_1 - 1, p_2 - 1, \ldots, p_k - 1$ est divisible par 5 (supposons que dans ce cas $p_1 - 1 \mathrel{\vdots} 5$). Dans le premier cas,

$p_1 - 1 = 4$, ce qui est impossible, car 10 n'est pas divisible par 4. Etant donné que p_1 doit être un nombre premier et que $10 : p_1 - 1$, le deuxième cas n'est possible que pour $p_1 = 11$. Mais alors $\alpha_1 = 1$, et il découle du théorème 21 que

$$\varphi\left(\frac{m}{11}\right) = 1,$$

c'est-à-dire ou bien $\frac{m}{11} = 1$, ou bien $\frac{m}{11} = 2$.

En définitive, on a $m_1 = 11$, $m_2 = 22$.

b) $p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1) = 8.$

Si m est impair, alors $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$ (car le deuxième membre de l'égalité écrite est la puissance de 2):

$$(p_1 - 1)(p_2 - 1)\ldots(p_k - 1) = 8.$$

Cela n'est possible que pour $k = 2$, $p_1 = 3$, $p_2 = 5$, c'est-à-dire pour $m = 15$.

Supposons maintenant le nombre m pair. Posons, pour fixer les idées, $p_1 = 2$. Il est évident que, comme précédemment, $\alpha_2 = \ldots = \alpha_k = 1$, et l'on a

$$2^{\alpha-1}(p_2 - 1)\ldots(p_k - 1) = 8.$$

On a évidemment $\alpha \leqslant 4$. Si $\alpha = 1$, ce cas est analogue au cas considéré: l'égalité écrite n'est également possible que pour $k = 3$, $p_2 = 3$, $p_3 = 5$, c'est-à-dire pour $m = 30$.

Si $\alpha = 2$, alors $k = 2$, $p_2 = 5$ et $m = 20$.

Si $\alpha = 3$, alors $k = 2$, $p_2 = 3$ et $m = 24$.

Si, enfin, $\alpha = 4$, alors $k = 1$ et $m = 16$.

Le problème a donc pour solutions: $m_1 = 15$, $m_2 = 30$, $m_3 = 20$, $m_4 = 24$, $m_5 = 16$.

54. Supposons que

$$p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1) = 14.$$

Chacun des nombres de la forme $p_i - 1$ est soit l'unité, soit un nombre pair et ne peut donc être 7. Etant d'une unité inférieur à un nombre premier, il ne peut être égal à 14. Donc, l'un des nombres $p_i^{\alpha_i - 1}$ est un 7. Mais alors $p_i - 1 = 6$, tandis que 14 n'est pas divisible par 6.

55. Soit $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Considérons d'abord le cas où m est la puissance d'un nombre premier: $m = p^{\alpha}$. Pour qu'un nombre soit premier avec m, il faut et il suffit qu'il ne soit pas divisible par p. Mais parmi les nombres 0, 1, 2, . . ., $m - 1$ il y a en tout $\frac{m}{p}$ divisibles par p. En conséquence, cette suite contient

$$m - \frac{m}{p} = m\left(1 - \frac{1}{p}\right) = p^{\alpha}\left(1 - \frac{1}{p}\right) =$$
$$= p^{\alpha-1}(p-1) = \varphi(m)$$

nombres premiers avec p.

Notons maintenant que pour que a et m soient premiers entre eux, il faut et il suffit que le reste de la division de a par m soit premier avec a.

D'après ce que nous venons de montrer, le nombre des restes de la division par $p_i^{\alpha_i}$ qui sont premiers avec $p_i^{\alpha_i}$ est égal à $\varphi(p_i^{\alpha_i})$. Mais, comme nous l'avons établi au cours de la résolution du problème 40, l'égalité des restes de la division des nombres par tous les $p_i^{\alpha_i}$ entraîne la congruence modulo m de ces nombres et inversement. De plus, pour qu'un nombre soit premier avec m, il faut et il suffit qu'il soit premier avec chacun des nombres $p_i^{\alpha_i}$.

En conséquence, à chaque combinaison de restes de la division par $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, qui sont premiers avec les divisieurs correspondants, correspond exactement un reste modulo m premier avec m. Il nous reste à noter que le

nombre de telles combinaisons de restes est égal à $\varphi(p_1^{\alpha_1}) \times \times \varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}) = \varphi(m)$.

56. Le soin de résoudre ce problème est laissé au lecteur.

57. $n^{13} - n = n(n^{12} - 1)$. Mais

$$n^{12} = n^{\varphi(13)} = n^{2\varphi(7)} = n^{3\varphi(5)} = n^{6\varphi(3)} = n^{12\varphi(2)}.$$

Donc, on a soit $n \vdots p$, soit $n^{12} - 1 \vdots p$ pour $p = 2, 3, 5, 7, 13$. Il ne nous reste plus qu'à nous référer au théorème 16.

58. Le soin de trouver la solution de ce problème est laissé au lecteur.

59. Admettons que le plus grand commun diviseur des nombres a et b soit d. Si c n'est pas divisible par d, l'équation $ax + by = c$ n'a pas de solutions entières. Si, par contre, c est divisible par d, on peut simplifier les deux membres de l'équation par d, et on arrive au cas examiné précédemment.

60. Soient A et B tels que $aA + bB = 1$. Posons

$$x_t = cA + bt, \quad y_t = c\frac{1-aA}{b} - at,$$

auquel cas

$$ax_t + by_t = a(cA + bt) + b\left(c\frac{1-aA}{b} - at\right) =$$
$$= caA + abt + c(1 - aA) - abt = c,$$

et (x_t, y_t) est effectivement une solution de notre équation.

61. a) $x_t = 9 \cdot 5^5 + 7t = 28\,125 + 7t$,

$$y_t = 9\frac{1-5^6}{7} - 5t = -20\,088 - 5t.$$

Etant donné que, dans les expressions de x_t et y_t, les termes constants et les coefficients de t sont en quelque sorte « approximativement proportionnels », on peut espérer pouvoir représenter nos solutions à l'aide des nombres plus petits. En effet, on peut écrire

$$x_t = 6 + 7(t + 4017), \quad y_t = -3 - 5(t + 4017),$$

ou, en posant $t + 4017 = t'$, on a

$$x_{t'} = 6 + 7t', \quad y_{t'} = -3 - 5t'.$$

Notons que le procédé de résolution donné au problème 60 permet de se contenter de nombres plus petits, mais nécessite des calculs un peu plus compliqués.

b) Profitons de ce que 25 modulo 13 appartient à l'exposant 2. On peut écrire

$$x_t = 8 \cdot 25 + 13 = 200 + 13t,$$

$$y_t = 8\,\frac{1-25^2}{13} - 25t = -384 - 25t,$$

ou, après simplifications,

$$x_t = 5 + 13t', \quad y_{t'} = -9 - 25t'.$$

62. La condition c) est remplie automatiquement, et la condition d) découle du théorème 25.

63.

m	17	19	27	29	31	49
k'	12 (ou 5)	2	19	3	28 (ou—3)	5

64. Nous laissons au lecteur le soin de trouver la solution de ce problème.

Suite de Fibonacci

1. L'Antiquité fut riche en grands mathématiciens. Maintes réalisations de la science mathématique ancienne émerveillent toujours par la finesse d'esprit de leurs auteurs, et les noms d'Euclide, d'Archimède, d'Héron sont connus de toute personne cultivée.

Il en va autrement pour le Moyen Age. Les mathématiques moyenâgeuses se développaient très lentement et nous ont laissé peu de noms célèbres. Aussi l'anonymat des découvertes de la science mathématique du Moyen Age ne prend-t-il fin dans les cours scolaires qu'avec Viète (XVI[e] siècle).

Cela augmente d'autant l'intérêt de *Liber abacci*, un ouvrage du célèbre mathématicien italien Léonard de Pise, dit Leonardo Fibonacci (abréviation de *filius Bonacii*). Ce livre fut écrit en 1202, mais seule sa deuxième variante datant de 1228 nous est parvenue.

Liber abacci est un ouvrage volumineux qui réunit à peu près tout ce qu'on savait à l'époque sur l'arithmétique et l'algèbre et qui a marqué pendant plusieurs siècles le développement des mathématiques en Europe occidentale. En particulier, c'est ce livre qui a fait connaître aux Européens les chiffres indiens (dits « arabes »).

L'exposé du traité est illustré par un grand nombre de problèmes qui en occupent une partie importante.

Examinons le problème qu'on trouve pp. 123-124 du manuscrit de 1228.

« Combien de paires de lapins peut engendrer une seule paire pendant une année? »

« Quelqu'un a mis une paire de lapins dans un endroit entouré de murs pour savoir combien de paires de lapins naîtraient au cours d'une année, la nature des lapins étant telle que dès l'âge de deux mois une paire en engendre tous les mois une autre. Comme la première femelle met bas le premier mois, il faut doubler et tu as deux paires pour ce mois; l'une d'elles, à savoir la première, a également les petits

Une paire	1
Premier mois	2
Deuxième mois	3
Troisième mois	5
Quatrième mois	8
Cinquième mois	13
Sixième mois	21
Septième mois	34
Huitième mois	55
Neuvième mois	89
Dixième mois	144
Onzième mois	233
Douzième mois	377

le mois suivant, de sorte que le deuxième mois on a 3 paires; le mois suivant deux paires sur trois procréent, ce qui donne deux paires de plus et le nombre de paires de lapins s'élève à 5 le troisième mois ; 3 d'entre elles ont la descendance et les paires de lapins sont huit le quatrième mois ; sur ce nombre 5 engendrent 5 autres et l'on obtient le cinquième mois 13 paires (5 + 8 = 13) ; 5 femelles nées le cinquième mois ne lapinent pas, tandis que les huit autres mettent au monde encore 8 paires, de sorte que le sixième mois on a 21 paires 21 plus 13 paires nées le septième mois donnent 34 ; 34 plus 21 paires nées le huitième mois donnent 55 ; 55 plus 34 paires nées le neuvième mois donnent 89 ; 89 plus 55 paires venues au monde le dixième mois donnent 144 paires ; celles-ci plus 89 paires engendrées le onzième mois donnent 233 paires ; 233 plus 144 paires nées le dernier mois donnent 377 ; tel est le nombre de paires de lapins engendrées par la paire de départ dans l'endroit donné douze mois plus tard. Le tableau ci-contre montre comment nous procédons, à savoir nous ajoutons le premier nombre au deuxième, c'est-à-dire 1 et 2, le deuxième au troisième, le troisième au quatrième, et ainsi de suite jusqu'à ce que nous ajoutons le dixième nombre au onzième, c'est-à-dire 144 et 233, et obtenons le nombre total de paires de lapins, c'est-à-dire

377; on peut continuer cette opération à l'infini. »

2. Passons maintenant des lapins aux nombres et considérons la suite numérique suivante:

$$u_1,\ u_2,\ \ldots,\ u_n, \tag{1}$$

où chaque terme est égal à la somme des deux termes immédiatement précédents, c'est-à-dire que pour tout $n > 2$, on a

$$u_n = u_{n-1} + u_{n-2}. \tag{2}$$

Les suites dont chaque terme est défini comme une fonction des termes précédents sont assez fréquentes en mathématiques; on les appelle *suites récurrentes.* On dit que les éléments d'une telle suite sont déterminés *par récurrence* et l'égalité (2) est la *relation de récurrence*. Le lecteur pourra trouver des éléments de la théorie générale des suites récurrentes dans la brochure de A. Markouchévitch « Quatre cours de mathématiques » (Editions de Moscou).

Remarquons avant tout que la condition (2) ne suffit pas à elle seule à déterminer les termes de la suite (1). On peut écrire une infinité de suites numériques distinctes vérifiant cette condition; par exemple,

$$2,\ 5,\ 7,\ 12,\ 19,\ 31,\ 50,\ \ldots,$$
$$1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ \ldots,$$
$$-1,\ -5,\ -6,\ -11,\ -17,\ \ldots,\ \text{etc.}$$

Ainsi, pour que la suite (1) soit déterminée de façon unique, la condition (2) est manifestement insuffisante; on doit donc introduire des conditions supplémentaires. On peut, par exemple, se donner quelques premiers termes de la suite (1). Combien doivent-ils être pour pouvoir calculer tous les termes suivants à l'aide de la seule condition (2)?

Disons pour commencer que tout terme de la suite (1) ne peut être obtenu à l'aide de (2), ne serait-ce parce qu'il n'est pas nécessairement précédé de deux autres; par exemple, le premier terme de la suite n'a pas de terme précédent et le deuxième n'en a qu'un seul. Donc, en plus de la condi-

tion (2), on doit encore savoir les deux premiers termes de la suite (1).

Il est évident que cela suffit pour pouvoir calculer tout terme de cette suite. En effet, u_3 peut être calculé comme la somme des deux termes donnés u_1 et u_2 ; u_4 comme la somme de u_2 et du terme déjà calculé u_3; u_5 comme la somme des termes déjà calculés u_3 et u_4, etc., à l'infini. En passant de cette façon de deux termes consécutifs de la suite au terme immédiatement suivant, on peut aboutir à un terme de numéro donné à l'avance et le calculer.

3. Considérons maintenant un cas particulier important de la suite (1) en posant $u_1 = 1$ et $u_2 = 1$. La condition (2) nous permet, on l'a vu, de calculer successivement tous les termes de cette suite. On peut vérifier facilement que les quatorze premiers termes de la suite en question sont les nombres 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, déjà rencontrés dans le problème de Fibonacci sur les lapins. La suite (1) avec $u_1 = u_2 = 1$ est donc appelée la *suite de Fibonacci*.

Les termes de la suite de Fibonacci (*nombres de Fibonacci*) jouissent de nombreuses propriétés curieuses fort importantes.

§ 1 PREMIÈRES PROPRIÉTÉS DES NOMBRES DE FIBONACCI

1. Calculons tout d'abord la somme de n premiers termes de la suite de Fibonacci. Plus précisément, démontrons que

$$u_1 + u_2 + \dots + u_n = u_{n+2} - 1. \qquad (1.1)$$

En effet, on a:

$$\begin{aligned} u_1 &= u_3 - u_2, \\ u_2 &= u_4 - u_3, \\ u_3 &= u_5 - u_4, \\ &\dots\dots\dots \\ u_{n-1} &= u_{n+1} - u_n, \\ u_n &= u_{n+2} - u_{n+1}. \end{aligned}$$

En additionnant membre à membre, on obtient

$$u_1 + u_2 + \ldots + u_n = u_{n+2} - u_2$$

et pour en déduire (1.1) il suffit de se rappeler que $u_2 = 1$.

2. La somme des termes de la suite de Fibonacci aux numéros impairs:

$$u_1 + u_3 + u_5 + \ldots + u_{2n-1} = u_{2n}. \tag{1.2}$$

Pour démontrer cette égalité écrivons

$$\begin{aligned} u_1 &= u_2, \\ u_3 &= u_4 - u_2, \\ u_5 &= u_6 - u_4, \\ &\ldots\ldots\ldots\ldots \\ u_{2n-1} &= u_{2n} - u_{2n-2}. \end{aligned}$$

En additionnant membre à membre, nous obtenons le résultat cherché.

3. La somme des termes de la suite de Fibonacci aux numéros pairs:

$$u_2 + u_4 + \ldots + u_{2n} = u_{2n+1} - 1. \tag{1.3}$$

En vertu du n° 1 on a

$$u_1 + u_2 + u_3 + \ldots + u_{2n} = u_{2n+2} - 1;$$

en retranchant de cette égalité l'égalité (1.2), on obtient

$$u_2 + u_4 + \ldots + u_{2n} = u_{2n+2} - 1 - u_{2n} = u_{2n+1} - 1,$$

ce qu'il fallait démontrer.

Retranchons maintenant (1.3) de (1.2); on obtient

$$u_1 - u_2 + u_3 - u_4 + \ldots + u_{2n-1} - u_{2n} = -u_{2n-1} + 1. \tag{1.4}$$

Ajoutons ensuite u_{2n+1} aux deux membres de (1.4):

$$u_1 - u_2 + u_3 - u_4 + \ldots - u_{2n} + u_{2n+1} = u_{2n} + 1. \tag{1.5}$$

De (1.4) et (1.5) on déduit la formule suivante pour la

somme alternée des termes de la suite de Fibonacci:

$$u_1 - u_2 + u_3 - u_4 + \ldots + (-1)^{n+1}u_n = (-1)^{n+1}u_{n-1} + 1. \tag{1.6}$$

4. Les formules (1.1) et (1.2) ont été obtenues par addition membre à membre de plusieurs égalités évidentes. Un autre exemple en est fourni par la formule donnant la somme des carrés de n premiers termes de la suite de Fibonacci:

$$u_1^2 + u_2^2 + \ldots + u_n^2 = u_n u_{n+1}. \tag{1.7}$$

Pour cela remarquons que

$$u_k u_{k+1} - u_{k-1} u_k = u_k (u_{k+1} - u_{k-1}) = u_k^2.$$

En additionnant membre à membre les égalités suivantes:

$$u_1^2 = u_1 u_2,$$
$$u_2^2 = u_2 u_3 - u_1 u_2,$$
$$u_3^2 = u_3 u_4 - u_2 u_3,$$
$$\cdots\cdots\cdots\cdots$$
$$u_n^2 = u_n u_{n+1} - u_{n-1} u_n,$$

on obtient la formule (1.7).

5. De nombreuses relations entre les termes de la suite de Fibonacci sont plus faciles à démontrer par la méthode de l'induction complète.

Décrivons la méthode de l'induction complète (ou le raisonnement par récurrence). Pour démontrer qu'une proposition quelconque est vraie pour tout entier naturel, il suffit d'établir que:

a) elle est vraie pour le nombre 1;

b) si elle est vraie pour un entier naturel n quelconque, elle l'est pour $n + 1$.

Aussi toute démonstration par récurrence d'une proposition vraie pour tout entier naturel se fait-elle en deux temps.

La première partie (d'habitude assez simple) établit que la proposition que l'on démontre est vraie pour le nombre 1. Dans la deuxième (d'habitude plus compliquée), on suppose que la proposition que l'on démontre est vraie pour un entier naturel n (quelconque mais fixe) et l'on déduit de cette *hypothèse de récurrence* que la proposition en question est vraie aussi pour $n + 1$.

Parfois le raisonnement par récurrence fait passer « de tous les nombres plus petits que n à n ». Dans ce cas on n'a plus besoin de la première partie de la démonstration car, à proprement parler, la démonstration pour $n = 1$ n'est autre que le passage de « tous » les entiers positifs plus petits que 1 (qui n'existent pas) à 1.

C'est justement de cette façon qu'on démontre que tout entier naturel peut être décomposé en facteurs premiers.

Supposons que tous les entiers naturels inférieurs à un certain n puissent être décomposés en produit de facteurs premiers. Si n est un nombre premier, il est lui-même sa décomposition. Si, par contre, n est un nombre composé, par définition il peut être mis sous la forme d'un produit d'au moins deux facteurs: $n = n_1 n_2$ avec $n_1 \neq 1$ et $n_2 \neq 1$. Mais alors $n_1 < n$ et $n_2 < n$ et selon l'hypothèse de récurrence n_1 et n_2 sont tous les deux décomposables en facteurs premiers. Il en résulte que le nombre n est lui-même décomposable en facteurs premiers.

Une variante encore plus compliquée du raisonnement par récurrence sera utilisée dans la démonstration du théorème du n° 36, § 2.

6. La réalisation la plus simple de l'idée du raisonnement par récurrence dans le cas de la suite de Fibonacci est la définition même de cette suite. Comme on l'a vu dans l'Introduction, elle comprend l'indication des deux premiers termes de la suite de Fibonacci: $u_1 = 1$, $u_2 = 1$ et le passage de u_n et u_{n+1} à u_{n+2} donné par la relation de récurrence

$$u_n + u_{n+1} = u_{n+2}.$$

Il en résulte en particulier que si une suite numérique quelconque commence par deux unités et si chacun des termes suivants est la somme de deux termes immédiatement précédents, elle est la suite de Fibonacci.

A titre d'exemple examinons un problème appelé « problème du sauteur ».

Un sauteur saute dans la même direction sur une piste divisée en cases. Chaque saut le porte dans la case suivante ou une case plus loin. De combien de façons le sauteur peut-il se déplacer de $n - 1$ cases et, en particulier, de la première case à la n-ième? (Les façons de sauter sont considérées comme identiques si le sauteur passe par les mêmes cases.)

Désignons le nombre cherché par x_n. Il est évident que $x_1 = 1$ (car le passage de la première case à elle-même peut être réalisé d'une seule façon — ne pas sauter) et $x_2 = 1$ (le passage de la première case à la seconde est aussi unique : c'est un saut dans la case immédiatement suivante). Supposons que le sauteur veuille arriver dans la $(n + 2)$-ième case. Par définition, le nombre total de procédés possibles est en l'occurrence égal à x_{n+2}. Mais ces procédés sont divisés dès le début en deux classes : ceux qui commencent avec le saut dans la deuxième case et ceux qui commencent avec le saut dans la troisième case. Or, s'il est dans la deuxième case, le sauteur peut atteindre la $(n + 2)$-ième de x_{n+1} façons, et de x_n façons s'il est dans la troisième. Par conséquent, la suite numérique $x_1, x_2, \ldots, x_n, \ldots$ vérifie la relation de récurrence

$$x_n + x_{n+1} = x_{n+2}$$

et coïncide donc avec la suite de Fibonacci : $x_n = u_n$.

7. Démontrons, par récurrence sur m, la formule importante suivante :

$$u_{n+m} = u_{n-1}u_m + u_n u_{m+1}. \qquad (1.8)$$

Pour $m = 1$ la formule (1.8) prend la forme évidente : $u_{n+1} = u_{n-1}u_1 + u_n u_2$. Pour $m = 2$ elle est également vraie, car

$$u_{n+2} = u_{n-1}u_2 + u_n u_3 = u_{n-1} + 2u_n = \\ = u_{n-1} + u_n + u_n = u_{n+1} + u_n.$$

Supposons que la formule (1.8) soit vraie pour $m = k$ et pour $m = k + 1$ et démontrons qu'elle l'est alors pour $m = k + 2$.

Soit

$$u_{n+k} = u_{n-1}u_k + u_n u_{k+1} \text{ et } u_{n+k+1} = u_{n-1}u_{k+1} + u_n u_{k+2}.$$

En additionnant membre à membre ces deux égalités, on

obtient

$$u_{n+k+2} = u_{n-1}u_{k+2} + u_n u_{k+3},$$

ce qu'il fallait démontrer.

La formule (1.8) peut être facilement interprétée (et même démontrée) en termes du problème du sauteur.

En effet, le nombre total de façons dont le sauteur peut se déplacer de la première case à la $(n+m)$-ième est égal à u_{n+m}. Ceci étant, le sauteur peut sauter la n-ième case ou bien passer par elle.

Dans le premier cas il doit aller jusqu'à la $(n-1)$-ième case (il peut le faire de u_{n-1} façons), ensuite sauter dans la $(n+1)$-ième, puis se déplacer de $(n+m)-(n+1) = m-1$ cases restantes (ce qu'on peut faire de u_m façons). Par conséquent, il y a $u_{n-1}u_m$ façons de sauter de ce type. Dans le second cas le sauteur doit atteindre d'abord la n-ième case (cela est possible de u_n façons) et ensuite se déplacer jusqu'à la $(n+m)$-ième (par l'un des u_{m+1} moyens possibles). On voit que les moyens du second type sont $u_n u_{m+1}$ et la formule (1.8) est donc démontrée.

8. En posant dans la formule (1.8) $m = n$, on obtient

$$u_{2n} = u_{n-1}u_n + u_n u_{n+1},$$

ou

$$u_{2n} = u_n (u_{n-1} + u_{n+1}). \qquad (1.9)$$

Cette dernière égalité montre que u_{2n} est divisible par u_n. Dans le paragraphe suivant nous démontrerons une proposition beaucoup plus générale.

Comme

$$u_n = u_{n+1} - u_{n-1},$$

la formule (1.9) peut être récrite comme suit:

$$u_{2n} = (u_{n+1} - u_{n-1})(u_{n+1} + u_{n-1}),$$

ou

$$u_{2n} = u_{n+1}^2 - u_{n-1}^2,$$

ce qui veut dire que la différence des carrés de deux termes de la suite de Fibonacci, dont les numéros diffèrent de deux unités, est elle aussi un terme de la suite de Fibonacci.

De façon analogue (en posant $m = 2n$), on peut montrer que

$$u_{3n} = u_{n+1}^3 + u_n^3 - u_{n-1}^3.$$

9. La formule suivante nous sera utile dans la suite:

$$u_n^2 = u_{n-1}u_{n+1} + (-1)^{n+1}. \qquad (1.10)$$

Démontrons-la par récurrence sur n. Pour $n = 1$ elle prend la forme évidente:

$$u_2^2 = u_1 u_3 - 1.$$

Supposons maintenant la formule (1.10) démontrée pour n quelconque. Ajoutons $u_n u_{n+1}$ à ses deux membres. Il vient:

$$u_n^2 + u_n u_{n+1} = u_{n-1}u_{n+1} + u_n u_{n+1} + (-1)^{n+1},$$

ou

$$u_n (u_n + u_{n+1}) = u_{n+1} (u_{n-1} + u_n) + (-1)^{n+1},$$

ou encore

$$u_n u_{n+2} = u_{n+1}^2 + (-1)^{n+1},$$

ou finalement

$$u_{n+1}^2 = u_n u_{n+2} + (-1)^{n+2}.$$

La formule (1.10) est donc démontrée pour tout n.

10. Par des procédés analogues à ceux qu'on vient d'utiliser il est facile d'établir les propriétés suivantes de la suite de Fibonacci:

$$u_1u_2 + u_2u_3 + u_3u_4 + \ldots + u_{2n-1}u_{2n} = u_{2n}^2,$$

$$u_1u_2 + u_2u_3 + u_3u_4 + \ldots + u_{2n}u_{2n+1} = u_{2n+1}^2 - 1,$$

$$nu_1 + (n-1)u_2 + (n-2)u_3 + \ldots + 2u_{n-1} + u_n = \\ = u_{n+4} - (n+3),$$

$$u_1 + 2u_2 + 3u_3 + \ldots + nu_n = nu_{n+2} - u_{n+3} + 2.$$

La démonstration en est laissée au lecteur.

11. Les nombres que nous allons envisager sont aussi remarquables que les termes de la suite de Fibonacci ; il s'agit des *coefficients binomiaux.*

On appelle coefficients binomiaux les coefficients des puissances de x dans le développement de $(1+x)^n$:

$$(1+x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + \ldots + C_n^n x^n. \qquad (1.11)$$

Il est évident que les nombres C_n^k sont définis de façon unique pour tous les entiers positifs n et tous les entiers non négatifs k inférieurs ou égaux à n.

L'usage des coefficients binomiaux est fort commode dans de nombreux raisonnements mathématiques. Ainsi, ils nous seront utiles lors de l'étude des propriétés de la suite de Fibonacci. En outre, il y a une relation directe entre les coefficients binomiaux et les termes de cette suite, et nous allons mettre en évidence certaines lois communes à ces deux classes de nombres.

Etablissons quelques propriétés des coefficients binomiaux.

En posant $n = 1$ dans (1.11), on voit immédiatement que

$$C_1^0 = C_1^1 = 1 ;$$

d'autre part, on a le lemme suivant.

● LEMME. $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

● DÉMONSTRATION. On a

$$(1+x)^{n+1} = (1+x)^n (1+x),$$

ou, en vertu de la définition des coefficients binomiaux,

$$C_{n+1}^0 + C_{n+1}^1 x + C_{n+1}^2 x^2 + \ldots + C_{n+1}^{n+1} x^{n+1} =$$
$$= (C_n^0 + C_n^1 x + C_n^2 x^2 + \ldots + C_n^n x^n)(1+x) =$$
$$= C_n^0 + (C_n^0 + C_n^1)\, x + (C_n^1 + C_n^2)\, x^2 + \ldots +$$
$$+ (C_n^{n-1} + C_n^n)\, x^n + C_n^n x^{n+1}.$$

Par suite,

$$C_{n+1}^{0}=C_{n}^{0},$$
$$C_{n+1}^{1}=C_{n}^{0}+C_{n}^{1},$$
$$\cdots\cdots\cdots$$
$$C_{n+1}^{k+1}=C_{n}^{k}+C_{n}^{k+1},$$
$$\cdots\cdots\cdots$$
$$C_{n+1}^{n+1}=C_{n}^{n},$$

ce qu'il fallait démontrer.

Du lemme démontré il résulte que les coefficients binomiaux peuvent être calculés à l'aide d'un procédé de récurrence analogue à celui qui nous a servi lors du calcul des termes de la suite de Fibonacci, mais d'une nature beaucoup plus compliquée. Cela nous permet de démontrer par récurrence diverses propositions concernant les coefficients binomiaux.

12. Mettons les coefficients binomiaux sous la forme du tableau suivant, appelé *triangle de Pascal*:

$$
\begin{array}{l}
C_0^0 \\
C_1^0\ C_1^1 \\
C_2^0\ C_2^1\ C_2^2 \\
\cdots\cdots\cdots \\
C_n^0\ C_n^1\ C_n^2 \ldots C_n^n \\
\cdots\cdots\cdots
\end{array}
$$

c'est-à-dire

$$
\begin{array}{lllllll}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1 \\
1 & 4 & 6 & 4 & 1 \\
1 & 5 & 10 & 10 & 5 & 1 \\
1 & 6 & 15 & 20 & 15 & 6 & 1 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

On numérote les lignes du triangle de Pascal du haut en bas, en attribuant le rang 0 à la ligne supérieure qui contient un seul nombre 1.

Il découle de ce qui précède que les nombres extrêmes de chaque ligne du triangle de Pascal sont égaux à 1 et que tout autre nombre du triangle est la somme du nombre supérieur et du nombre supérieur gauche.

13. La formule (1.11) permet d'obtenir immédiatement deux relations importantes entre les coefficients binomiaux d'une même rangée horizontale du triangle de Pascal.

Si l'on pose $x = 1$ dans (1.11), on obtient

$$2^n = C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n.$$

Pour $x = -1$ on trouve

$$0 = C_n^0 - C_n^1 + C_n^2 + \ldots + (-1)^n C_n^n.$$

14. Appliquons l'induction complète par rapport à n pour démontrer que

$$C_n^k = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\cdot\ldots\cdot k}. \qquad (1.12)$$

Cette formule est souvent considérée comme la définition des coefficients binomiaux. Elle détermine le coefficient binomial C_n^k comme le nombre des combinaisons avec répétition de n lettres k à k. Nous avons préféré ici une voie plus formelle.

Si l'on convient de considérer tout produit de zéro facteurs comme égal à 1, en posant $k = 0$ dans (1.12), on obtient la relation déjà connue: $C_n^0 = 1$. Compte tenu de ce fait, on peut se borner au cas $k \geqslant 1$.

Pour $n = 1$ on a

$$C_1^1 = \frac{1}{1} = 1.$$

Supposons maintenant la formule (1.12) vraie pour une valeur quelconque de n et pour tout $k = 0, 1, \ldots, n$.

Considérons le nombre C_{n+1}^{k}. Comme $k \geqslant 1$, on peut écrire

$$C_{n+1}^{k} = C_n^{k-1} + C_n^{k},$$

ou, en utilisant l'hypothèse de récurrence (1.12),

$$C_n^{k-1} + C_n^{k} = \frac{n(n-1)\ldots(n-k+2)}{1\cdot 2\cdot\ldots\cdot(k-1)} +$$
$$+ \frac{n(n-1)\ldots(n-k+2)(n-k+1)}{1\cdot 2\cdot\ldots\cdot(k-1)k} =$$
$$= \frac{n(n-1)\ldots(n-k+2)}{1\cdot 2\cdot\ldots\cdot(k-1)}\left(1 + \frac{n-k+1}{k}\right) =$$
$$= \frac{n(n-1)\ldots(n-k+2)}{1\cdot 2\cdot\ldots\cdot(k-1)}\,\frac{k+n-k+1}{k} =$$
$$= \frac{(n+1)\,n(n-1)\ldots(n-k+2)}{1\cdot 2\cdot\ldots\cdot(k-1)k} = C_{n+1}^{k}.$$

Cette dernière égalité n'est autre que la formule (1.12) pour la rangée suivante, c'est-à-dire la $(n+1)$-ième, du triangle de Pascal.

15. Menons par les nombres du triangle de Pascal des droites formant des angles de 45° avec ses lignes (telles sont, par exemple, les droites passant par les nombres 1, 4, 3 ou 1, 5, 6, 1).

Montrons que la somme des nombres d'une ligne oblique quelconque est un terme de la suite de Fibonacci.

En effet, la première ligne oblique est formée d'un seul nombre 1. Il en est de même pour la deuxième. Pour démontrer la proposition en question il suffit de montrer que la somme de tous les nombres de la n-ième et de la $(n+1)$-ième ligne oblique est égale à la somme des nombres de la $(n+2)$-ième.

Or, les nombres de la n-ième et de la $(n+1)$-ième ligne oblique sont respectivement

$$C_{n-1}^{0},\ C_{n-2}^{1},\ C_{n-3}^{2},\ \ldots$$

et

$$C_{n}^{0},\ C_{n-1}^{1},\ C_{n-2}^{2},\ \ldots$$

Leur somme s'écrit:

$$C_n^0 + (C_{n-1}^0 + C_{n-1}^1) + (C_{n-2}^1 + C_{n-2}^2) + \ldots,$$

ou, compte tenu du lemme du nº 11,

$$C_{n+1}^0 + C_n^1 + C_{n-1}^2 + \ldots$$

Mais cette dernière expression représente la somme des nombres de la $(n+2)$-ième ligne oblique du triangle de Pascal.

La proposition démontrée donne immédiatement, à l'aide de la formule (1.1), le résultat suivant: la somme de tous les coefficients binomiaux situés au-dessus de la n-ième ligne oblique du triangle de Pascal (y compris cette dernière) est égale à $u_{n+2} - 1$.

En utilisant les formules (1.2), (1.3), (1.4), etc., le lecteur obtiendra sans peine d'autres relations entre les termes de la suite de Fibonacci et les coefficients binomiaux.

16. Jusqu'à présent on définissait les termes de la suite de Fibonacci par récurrence sur leurs numéros. Il se trouve pourtant que tout terme de la suite de Fibonacci peut être défini comme une fonction explicite de son numéro.

Pour le démontrer étudions différentes suites u_1, u_2, ..., u_n, ..., vérifiant la relation

$$u_n = u_{n-2} + u_{n-1}, \qquad (1.13)$$

et appelons-les *solutions de l'équation* (1.13).

Les lettres V, V' et V'' désigneront les suites

$$v_1, v_2, v_3, \ldots$$
$$v_1', v_2', v_3', \ldots$$
$$v_1'', v_2'', v_3'', \ldots$$

Démontrons d'abord deux lemmes simples.

● LEMME 1. *Si V est une solution de l'équation* (1.13) *et c un nombre quelconque, la suite cV (c'est-à-dire la suite cv_1, cv_2, cv_3, ...) est elle aussi une solution de l'équation* (1.13).

● DÉMONSTRATION. En multipliant tous les termes de l'égalité

$$v_n = v_{n-1} + v_{n-2}$$

par c, on obtient

$$cv_n = cv_{n-2} + cv_{n-1},$$

ce qu'il fallait démontrer.

● LEMME 2. *Si les suites V' et V'' sont des solutions de l'équation* (1.13), *leur somme $V' + V''$ (c'est-à-dire la suite $v'_1 + v''_1$, $v'_2 + v''_2$, $v'_3 + v''_3$, . . .) est elle aussi une solution de l'équation* (1.13).

● DÉMONSTRATION. On a par hypothèse

$$v'_n = v'_{n-1} + v'_{n-2}$$

et

$$v''_n = v''_{n-1} + v''_{n-2}.$$

En additionnant membre à membre, on obtient:

$$v'_n + v''_n = (v'_{n-1} + v''_{n-1}) + (v'_{n-2} + v''_{n-2}),$$

ce qui démontre le lemme.

Soient à présent V' et V'' deux solutions non proportionnelles de l'équation (1.13) $\left(\text{c'est-à-dire deux solutions telles que pour tout } c \text{ constant on peut trouver un numéro } n \text{ pour lequel } \frac{v'_n}{v''_n} \neq c\right)$. Montrons que toute suite V, solution de l'équation (1.13), peut être mise sous la forme

$$c_1V' + c_2V'', \tag{1.14}$$

où c_1 et c_2 sont des constantes. On dit que (1.14) est la *solution générale* de l'équation (1.13).

Démontrons préalablement que si les solutions V' et V'' de l'équation (1.13) ne sont pas proportionnelles, on a

$$\frac{v'_1}{v''_1} \neq \frac{v'_2}{v''_2} \tag{1.15}$$

(c'est-à-dire que cette non-proportionnalité a lieu dès les deux premiers termes des suites V' et V'').

On démontre (1.15) par l'absurde. Supposons que pour les solutions non proportionnelles V' et V'' de l'équation (1.13) on ait

$$\frac{v_1'}{v_1''} = \frac{v_2'}{v_2''}. \tag{1.16}$$

En écrivant la proportion dérivée, on obtient

$$\frac{v_1' + v_2'}{v_1'' + v_2''} = \frac{v_2'}{v_2''}$$

ou bien, vu que V' et V'' sont des solutions de l'équation (1.13),

$$\frac{v_3'}{v_3''} = \frac{v_2'}{v_2''}.$$

On voit de manière analogue (l'induction!) que

$$\frac{v_3'}{v_3''} = \frac{v_4'}{v_4''} = \ldots = \frac{v_n'}{v_n''} = \ldots$$

Ainsi, il résulte de (1.16) que les suites V' et V'' sont proportionnelles, ce qui contredit l'hypothèse. Donc, la relation (1.15) est vraie.

Considérons maintenant une suite quelconque V qui soit solution de l'équation (1.13). Comme cela a été montré au nº 2 de l'Introduction, une telle suite est bien déterminée si l'on se donne ses deux premiers termes v_1 et v_2.

Cherchons deux constantes c_1 et c_2 telles qu'on ait

$$\begin{aligned} c_1 v_1' + c_2 v_1'' &= v_1, \\ c_1 v_2' + c_2 v_2'' &= v_2. \end{aligned} \tag{1.17}$$

Alors, d'après les lemmes 1 et 2, la suite V ne sera autre que $c_1 V' + c_2 V''$.

En vertu de la condition (1.15), le système d'équations (1.17) est résoluble par rapport à c_1 et c_2 quels que soient les nombres v_1 et v_2:

$$c_1 = \frac{v_1 v_2'' - v_2 v_1''}{v_1' v_2'' - v_1'' v_2'}, \qquad c_2 = \frac{v_1' v_2 - v_2' v_1}{v_1' v_2'' - v_1'' v_2'}.$$

(La condition (1.15) signifie que le dénominateur commun de ces deux fractions est différent de zéro.) En remplaçant dans (1.14) c_1 et c_2 par leurs valeurs ainsi trouvées, on obtient la représentation cherchée de la suite V.

Ainsi, pour décrire l'ensemble de *toutes* les solutions de l'équation (1.13), il suffit de trouver ses *deux* solutions non proportionnelles quelconques.

On va chercher ces solutions parmi les progressions géométriques. Conformément au lemme 1, on peut se borner aux progressions dont le premier terme est égal à 1. Soit donc une telle progression:

$$1, q, q^2, \ldots$$

Pour qu'elle soit une solution de l'équation (1.13), il faut que pour tout n on ait

$$q^{n-2} + q^{n-1} = q^n;$$

ou, en simplifiant par q^{n-2},

$$1 + q = q^2. \qquad (1.18)$$

Les racines de cette équation du second degré, c'est-à-dire les nombres $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$, sont justement les raisons des progressions cherchées. Désignons-les respectivement par α et β. Il faut souligner que les nombres α et β, en tant que racines de l'équation (1.18), doivent vérifier les relations $1 + \alpha = \alpha^2$, $1 + \beta = \beta^2$ et $\alpha\beta = -1$.

Ainsi, nous avons trouvé deux progressions géométriques qui sont des solutions de l'équation (1.13). Donc, toutes les suites de la forme

$$c_1 + c_2, \; c_1\alpha + c_2\beta, \; c_1\alpha^2 + c_2\beta^2, \ldots \qquad (1.19)$$

sont des solutions de l'équation (1.13). Les progressions trouvées étant de raisons différentes, donc non proportionnelles, on obtient de la formule (1.19), pour des valeurs différentes de c_1 et c_2, toutes les solutions de l'équation (1.13).

En particulier, pour certaines valeurs de c_1 et c_2 la formule (1.19) nous donne également la suite de Fibonacci. Pour cela, comme on l'a indiqué plus haut, il faut déterminer c_1 et c_2 des équations

$$c_1 + c_2 = u_1$$

et

$$c_1\alpha + c_2\beta = u_2,$$

c'est-à-dire du système

$$c_1 + c_2 = 1,$$

$$c_1 \frac{1+\sqrt{5}}{2} + c_2 \frac{1-\sqrt{5}}{2} = 1.$$

En résolvant ce système, on obtient

$$c_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}, \quad c_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}},$$

d'où

$$u_n = c_1\alpha^{n-1} + c_2\beta^{n-1} =$$

$$= \frac{1+\sqrt{5}}{2\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1-\sqrt{5}}{2\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{n-1},$$

c'est-à-dire

$$u_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}. \qquad (1.20)$$

La formule (1.20) s'appelle la *formule de Binet*.

Evidemment, on peut obtenir des formules analogues pour d'autres solutions de (1.13). Le lecteur est invité de le faire pour les suites données au n° 2 de l'Introduction.

17. Nous avons vu que $\alpha^2 = \alpha + 1$. Il est donc clair que toute puissance entière positive du nombre α peut être mise sous la forme $a\alpha + b$ avec des coefficients entiers a et b.

Ainsi,

$\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 2\alpha + 1,$
$\alpha^4 = \alpha\alpha^3 = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha = 2\alpha + 2 + \alpha = 3\alpha + 2,$
etc.

Démontrons (par récurrence) que

$$\alpha^n = u_n\alpha + u_{n-1}.$$

En effet, pour $n = 2, 3$ cette formule est vraie. Supposons que

$$\alpha^k = u_k\alpha + u_{k-1},$$
$$\alpha^{k+1} = u_{k+1}\alpha + u_k.$$

En additionnant ces deux égalités, on obtient

$$\alpha^k + \alpha^{k+1} = (u_k + u_{k+1})\,\alpha + (u_{k-1} + u_k),$$

ou

$$\alpha^{k+2} = u_{k+2}\alpha + u_{k+1},$$

ce qui achève le raisonnement.

18. La formule de Binet facilite la sommation de nombreuses séries liées aux termes de la suite de Fibonacci.

Cherchons, par exemple, la somme

$$u_3 + u_6 + u_9 + \ldots + u_{3n}.$$

On a

$$u_3 + u_6 + \ldots + u_{3n} = \frac{\alpha^3 - \beta^3}{\sqrt{5}} + \frac{\alpha^6 - \beta^6}{\sqrt{5}} + \ldots + \frac{\alpha^{3n} - \beta^{3n}}{\sqrt{5}} =$$
$$= \frac{1}{\sqrt{5}}(\alpha^3 + \alpha^6 + \ldots + \alpha^{3n} - \beta^3 - \beta^6 - \ldots - \beta^{3n}),$$

ou, en faisant la somme des progressions,

$$u_3 + u_6 + \ldots + u_{3n} = \frac{1}{\sqrt{5}}\left(\frac{\alpha^{3n+3} - \alpha^3}{\alpha^3 - 1} - \frac{\beta^{3n+3} - \beta^3}{\beta^3 - 1}\right).$$

Mais

$$\alpha^3 - 1 = \alpha + \alpha^2 - 1 = \alpha + \alpha + 1 - 1 = 2\alpha$$

et, de même, $\beta^3 - 1 = 2\beta$. Donc,

$$u_3 + u_6 + \ldots + u_{3n} = \frac{1}{\sqrt{5}}\left(\frac{\alpha^{3n+3} - \alpha^3}{2\alpha} - \frac{\beta^{3n+3} - \beta^3}{2\beta}\right).$$

ou, après simplifications,

$$u_3+u_6+\ldots+u_{3n}=\frac{1}{\sqrt{5}}\left(\frac{\alpha^{3n+2}-\alpha^2-\beta^{3n+2}+\beta^2}{2}\right)=$$

$$=\frac{1}{2}\left(\frac{\alpha^{3n+2}-\beta^{3n+2}}{\sqrt{5}}-\frac{\alpha^2-\beta^2}{\sqrt{5}}\right)=\frac{1}{2}(u_{3n+2}-u_2)=\frac{u_{3n+2}-1}{2}.$$

19. Un autre exemple d'application de la formule de Binet est donné par le calcul de la somme des cubes de n premiers termes de la suite de Fibonacci.

Remarquons d'abord que

$$u_k^3=\left(\frac{\alpha^k-\beta^k}{\sqrt{5}}\right)^3=\frac{1}{5}\,\frac{\alpha^{3k}-3\alpha^{2k}\beta^k+3\alpha^k\beta^{2k}-\beta^{3k}}{\sqrt{5}}=$$

$$=\frac{1}{5}\left(\frac{\alpha^{3k}-\beta^{3k}}{\sqrt{5}}-3\alpha^k\beta^k\,\frac{\alpha^k-\beta^k}{\sqrt{5}}\right)=$$

$$=\frac{1}{5}(u_{3k}-(-1)^k\,3u_k)=\frac{1}{5}(u_{3k}+(-1)^{k+1}\,3u_k).$$

On a donc

$$u_1^3+u_2^3+\ldots+u_n^3=\frac{1}{5}[(u_3+u_6+\ldots+u_{3n})+$$

$$+3(u_1-u_2+u_3-\ldots+(-1)^{n+1}u_n)],$$

d'où, à l'aide de la formule (1.6) et des résultats du numéro précédent, on obtient

$$u_1^3+u_2^3+\ldots+u_n^3=\frac{1}{5}\left(\frac{u_{3n+2}-1}{2}+(-1)^{n+1}\,3u_{n-1}\right)=$$

$$=\frac{u_{3n+2}+(-1)^{n+1}\,6u_{n-1}-1}{10}.$$

20. Il est naturel de s'intéresser à la rapidité de croissance des termes de la suite de Fibonacci avec leurs numéros. La formule de Binet nous fournit une fois de plus une réponse exhaustive.

Il est facile de démontrer le théorème suivant:

● THÉORÈME. *Le terme u_n de la suite de Fibonacci est l'entier le plus proche du nombre $\frac{\alpha^n}{\sqrt{5}}$, c'est-à-dire du terme*

n-ième a_n de la progression géométrique dont le premier terme est $\frac{\alpha}{\sqrt{5}}$ et la raison est égale à α.

● DÉMONSTRATION. Il suffit évidemment de démontrer que la différence $u_n - a_n$ est toujours inférieure à $\frac{1}{2}$ en valeur absolue. Mais

$$|u_n - a_n| = \left|\frac{\alpha^n - \beta^n}{\sqrt{5}} - \frac{\alpha^n}{\sqrt{5}}\right| = \left|\frac{\alpha^n - \alpha^n - \beta^n}{\sqrt{5}}\right| = \frac{|\beta|^n}{\sqrt{5}}.$$

Comme $\beta = -0{,}68\ldots$, on a $|\beta| < 1$, donc $|\beta|^n < 1$, quel que soit n ; à plus forte raison, $\frac{|\beta|}{\sqrt{5}} < \frac{1}{2}$ (car $\sqrt{5} > 2$). Le théorème est démontré.

En modifiant convenablement la démonstration de ce théorème, le lecteur qui connaît la théorie des limites peut montrer sans difficulté que

$$\lim_{n \to \infty} |u_n - a_n| = 0.$$

En utilisant le théorème démontré, on peut calculer les termes de la suite de Fibonacci à l'aide des tables de logarithmes.

Calculons, par exemple, u_{14} (il est clair que u_{14} doit être la réponse au problème de Fibonacci sur les lapins) :

$$\sqrt{5} = 2{,}2361, \qquad \lg\sqrt{5} = 0{,}34949\,;$$

$$\alpha = \frac{1+\sqrt{5}}{2} = 1{,}6180, \quad \lg\alpha = 0{,}20898\,;$$

$$\lg\frac{\alpha^{14}}{\sqrt{5}} = 14\cdot 0{,}20898 - 0{,}34949 = 2{,}5762,$$

$$\frac{\alpha^{14}}{\sqrt{5}} = 376{,}9.$$

L'entier le plus proche de 376,9 est 377 ; c'est bien u_{14}.

Si les termes de la suite de Fibonacci que l'on veut calculer possèdent de grands numéros, nous ne pouvons trouver à l'aide des tables de logarithmes que quelques premiers chiffres du nombre ; dans ce cas, le calcul est donc approché.

A titre d'exercice le lecteur pourra démontrer que dans le système de numération décimale le nombre des chiffres de u_n pour $n \geqslant 17$ est compris entre $\frac{n}{5}$ et $\frac{n}{4}$. En particulier, quel est le nombre de chiffres de u_{1000}?

21. Le résultat du numéro précédent peut être rendu plus précis. Le théorème suivant nous sera utile dans la suite.

● THÉORÈME.
$$\frac{\alpha^{n-\frac{1}{n}}}{\sqrt{5}} \leqslant u_n \leqslant \frac{\alpha^{n+\frac{1}{n}}}{\sqrt{5}}.$$

● DÉMONSTRATION. Nous ne démontrerons que la première inégalité : la deuxième se démontre de façon analogue.

D'après la formule de Binet on a

$$u_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n);$$

d'autre part, $\alpha\beta = -1$. Donc, il nous suffit de démontrer que

$$\alpha^{n-\frac{1}{n}} \leqslant \alpha^n - \frac{1}{\alpha^n},$$

ou

$$\alpha^{2n-\frac{1}{n}} \leqslant \alpha^{2n} - 1,$$

ou encore, en élevant les deux membres à la puissance n,

$$\alpha^{2n^2-1} \leqslant (\alpha^{2n} - 1)^n. \qquad (1.21)$$

Nous allons démontrer cette inégalité par récurrence. Pour $n = 1$ elle prend la forme

$$\alpha \leqslant \alpha^2 - 1,$$

qui est évidemment vraie (notamment pour le signe d'égalité). Pour $n = 2$ (1.21) devient

$$\alpha^7 \leqslant (\alpha^4 - 1)^2. \qquad (1.22)$$

Cette inégalité peut être vérifiée par le calcul direct. Mais on peut également recourir à la relation établie au nº 17. Dans notre cas on a

$$\alpha^4 = 3\alpha + 2,$$

$$(\alpha^4 - 1)^2 = (3\alpha + 1)^2 = 9\alpha^2 + 6\alpha + 1 = 15\alpha + 10$$

et l'inégalité (1.22) se récrit:

$$\alpha^7 = 13\alpha + 8 \leqslant 15\alpha + 10,$$

ce qui est évident. Enfin, pour $n = 3$ l'inégalité (1.21) prend la forme

$$\alpha^{17} \leqslant (\alpha^6 - 1)^3,$$

qui peut être vérifiée comme ci-dessus.

Supposons maintenant que $n > 2$ et que l'inégalité (1.21) soit remplie; montrons que

$$\alpha^{2(n+1)^2-1} \leqslant (\alpha^{2n+2} - 1)^{n+1}.$$

Pour cela il suffit de montrer que lorsque n augmente d'une unité, le premier membre de (1.21) croît moins vite que le second. Or, il est évident que le premier membre augmente α^{4n+2} fois. Evaluons l'augmentation du second.

On a

$$\frac{(\alpha^{2(n+1)} - 1)^{n+1}}{(\alpha^{2n} - 1)^n} = (\alpha^{2(n+1)} - 1)\left(\frac{\alpha^{2(n+1)} - 1}{\alpha^{2n} - 1}\right)^n.$$

La dernière fraction est supérieure à α^2 de

$$\frac{\alpha^{2(n+1)} - 1}{\alpha^{2n} - 1} - \alpha^2 = \frac{\alpha^{2n+2} - 1 - \alpha^{2n+2} + \alpha^2}{\alpha^{2n} - 1} =$$

$$= \frac{\alpha^2 - 1}{\alpha^{2n} - 1} = \frac{1}{\alpha^{2n-2} + \alpha^{2n-4} + \ldots + \alpha^2 + 1} > \frac{1}{\alpha^{2n-1}}.$$

Par conséquent,

$$\left(\frac{\alpha^{2(n+1)} - 1}{\alpha^{2n} - 1}\right)^n > \left(\alpha^2 + \frac{1}{\alpha^{2n-1}}\right)^n = \alpha^{2n} + n\,\frac{\alpha^{2n-2}}{\alpha^{2n-1}} + \ldots,$$

où les points de suspension remplacent des termes positifs.

Etant donné que $n > 2$, l'expression ci-dessus est plus grande que α^{2n+1}. Donc,

$$\frac{(\alpha^{2(n+1)} - 1)^{n+1}}{(\alpha^{2n} - 1)^n} > (\alpha^{2(n+1)} - 1)(\alpha^{2n} + 1) =$$

$$= \alpha^{4n+2} + \alpha^{2n+2} - \alpha^{2n} - 1 = \alpha^{4n+2} + \alpha^{2n}(\alpha^2 - 1) - 1 =$$

$$= \alpha^{4n+2} + \alpha^{2n+1} - 1 > \alpha^{4n+2}.$$

Le théorème est démontré.

22. Considérons encore une classe de suites fondées sur les propriétés des termes de la suite de Fibonacci. Soit x un nombre quelconque. Calculons la somme

$$s_n(x) = u_1x + u_2x^2 + \ldots + u_nx^n.$$

Pour cela utilisons tout d'abord la formule de Binet:

$$s_n(x) = \frac{\alpha-\beta}{\sqrt{5}}x + \frac{\alpha^2-\beta^2}{\sqrt{5}}x^2 + \ldots + \frac{\alpha^n-\beta^n}{\sqrt{5}}x^n =$$

$$= \frac{1}{\sqrt{5}}(\alpha x + \alpha^2x^2 + \ldots + \alpha^nx^n) -$$

$$- \frac{1}{\sqrt{5}}(\beta x + \beta^2x^2 + \ldots + \beta^nx^n). \quad (1.23)$$

Les expressions entre parenthèses sont les sommes de deux progressions géométriques de raisons respectives αx et βx. La formule connue pour le calcul de la somme d'une progression géométrique n'est valable que si la raison est différente de 1. Dans le cas contraire, tous les termes de la progression sont égaux entre eux et le calcul de leur somme ne présente aucune difficulté.

Conformément à ce qu'on vient de dire, considérons d'abord le cas où $\alpha x \neq 1$ et $\beta x \neq 1$, c'est-à-dire $x \neq \frac{1}{\alpha} = -\beta$ et $x \neq \frac{1}{\beta} = -\alpha$. En calculant dans (1.23) les sommes des progressions géométriques, on obtient

$$s_n(x) = \frac{1}{\sqrt{5}}\frac{\alpha^{n+1}x^{n+1}-\alpha x}{\alpha x-1} - \frac{1}{\sqrt{5}}\frac{\beta^{n+1}x^{n+1}-\beta x}{\beta x-1}$$

ou, en réduisant les fractions au même dénominateur,

$$s_n(x) = \frac{1}{\sqrt{5}}\frac{(\alpha^{n+1}x^{n+1}-\alpha x)(\beta x-1)-(\beta^{n+1}x^{n+1}-\beta x)(\alpha x-1)}{(\alpha x-1)(\beta x-1)} =$$

$$= \frac{1}{\sqrt{5}}\frac{\alpha^{n+1}\beta x^{n+2}-\alpha^{n+1}x^{n+1}+\alpha x}{\alpha\beta x^2-(\alpha+\beta)x+1} -$$

$$- \frac{1}{\sqrt{5}}\frac{\alpha\beta^{n+1}x^{n+2}+\beta^{n+1}x^{n+1}-\beta x}{\alpha\beta x^2-(\alpha+\beta)x+1}.$$

Si l'on se souvient que $\alpha\beta = -1$, $\alpha + \beta = 1$ et $\alpha - \beta = \sqrt{5}$, on peut écrire

$$s_n(x) = \frac{1}{\sqrt{5}} \frac{x\sqrt{5} - (\alpha^n - \beta^n)\, x^{n+2} - (\alpha^{n+1} - \beta^{n+1})\, x^{n+1}}{1 - x - x^2},$$

d'où

$$s_n(x) = \frac{x - u_n x^{n+2} - u_{n+1} x^{n+1}}{1 - x - x^2}. \tag{1.24}$$

En particulier, pour $x = 1$ cette formule donne

$$s_n(1) = u_1 + u_2 + \ldots + u_n = \frac{1 - u_n - u_{n+1}}{-1} = u_{n+2} - 1,$$

ce qui confirme le résultat du nº 1.

Pour $x = -1$ on a

$$s_n(-1) = u_1 - u_2 + \ldots + (-1)^{n-1} u_n =$$
$$= \frac{-1 - u_n(-1)^{n+2} - u_{n+1}(-1)^{n+1}}{-1} = (-1)^{n+1} u_{n-1} - 1$$

(cf. (1.6)).

Examinons maintenant les cas « particuliers ».

Soit $x = \frac{1}{\alpha} = -\beta$. Dans ce cas tous les termes de la première progression de (1.23) sont égaux à 1 ; donc, leur somme est égale à n. Quant à la deuxième progression, elle est de raison $-\beta^2$.

Ainsi,

$$s_n\left(\frac{1}{\alpha}\right) = \frac{1}{\sqrt{5}}\left(n - (\beta^2 - \beta^4 + \ldots + (-1)^{n-1}\beta^{2n})\right) =$$
$$= \frac{1}{\sqrt{5}}\left(n - \frac{\beta^2 - (-1)^n \beta^{2n+2}}{1 + \beta^2}\right) =$$
$$= \frac{1}{\sqrt{5}}\left(n - \frac{\beta^2}{1 + \beta^2} + (-1)^n \beta^{2n} \frac{\beta^2}{1 + \beta^2}\right).$$

Si l'on remarque que

$$1 + \beta^2 = 2 + \beta = 2 + \frac{1 - \sqrt{5}}{2} = \frac{5 - \sqrt{5}}{2}$$

et

$$\frac{\beta^2}{1+\beta^2}=\frac{1+\beta}{2+\beta}=\frac{3-\sqrt{5}}{5-\sqrt{5}}=\frac{(3-\sqrt{5})(5+\sqrt{5})}{(5-\sqrt{5})(5+\sqrt{5})}=\frac{10-2\sqrt{5}}{20},$$

on obtient

$$s_n\left(\frac{1}{\alpha}\right)=\frac{n}{\sqrt{5}}-\frac{5\sqrt{5}-5}{2}+(-1)^n\beta^{2n}\frac{5\sqrt{5}-5}{2}. \quad (1.25)$$

Enfin, soit $x=\frac{1}{\beta}$. Dans ce cas, c'est la deuxième progression de (1.23) qui est de raison 1, tandis que la première a pour raison $-\alpha^2$. On a donc

$$s_n\left(\frac{1}{\beta}\right)=\frac{1}{\sqrt{5}}((\alpha^2-\alpha^4+\ldots+(-1)^{n-1}\alpha^{2n})-n).$$

En procédant comme ci-dessus, on obtient

$$s_n\left(\frac{1}{\beta}\right)=\frac{1}{\sqrt{5}}\left(\frac{\alpha^2-(-1)^n\alpha^{2n+2}}{1+\alpha^2}-n\right)=$$

$$=\frac{1}{\sqrt{5}}\left((-1)^{n+1}\alpha^{2n}\frac{\alpha^2}{1+\alpha^2}+\frac{\alpha^2}{1+\alpha^2}-n\right),$$

d'où, en définitive,

$$s_n\left(\frac{1}{\beta}\right)=(-1)^{n+1}\frac{1+\sqrt{5}}{10}\alpha^{2n}+\frac{1+\sqrt{5}}{10}-\frac{n}{\sqrt{5}}. \quad (1.26)$$

23. Etudions maintenant le comportement de la somme $s_n(x)$ pour x fixe et n indéfiniment croissant.

En passant dans l'égalité (1.23) à la limite par rapport à n, on obtient

$$\lim_{n\to\infty}s_n(x)=\lim_{n\to\infty}\frac{1}{\sqrt{5}}((\alpha x+\alpha^2x^2+\ldots+\alpha^nx^n)-$$

$$-(\beta x+\beta^2x^2+\ldots+\beta^nx^n))=$$

$$=\frac{1}{\sqrt{5}}\lim_{n\to\infty}(\alpha x+\alpha^2x^2+\ldots+\alpha^nx^n)-$$

$$-\frac{1}{\sqrt{5}}\lim_{n\to\infty}(\beta x+\beta^2x^2+\ldots+\beta^nx^n).$$

On a sous les deux derniers signes de limites des sommes de progressions géométriques. Aussi les limites elles-mêmes sont égales aux sommes des progressions géométriques infinies correspondantes. Or, comme on le sait, pour pouvoir parler de la somme d'une progression géométrique infinie, il faut et il suffit que sa raison soit inférieure à 1 en valeur absolue. Les progressions considérées ont pour raisons αx et βx. Comme $|\alpha| > |\beta|$, $|\alpha x| < 1$ entraîne $|\beta x| < 1$. Ainsi, si l'inégalité $|\alpha x| < 1$ est satisfaite, toutes les limites qui nous intéressent à l'instant donné existent.

Ainsi, la limite

$$\lim_{n\to\infty} s_n(x) \tag{1.27}$$

existe si $|x| < \frac{1}{\alpha}$. Désignons cette limite par $s(x)$. Pour son calcul on peut se servir de la formule (1.24).

Remarquons à cette fin que conformément au théorème du nº 20 on a

$$u_n \leqslant \frac{\alpha^n}{\sqrt{5}} + 1.$$

C'est pourquoi

$$\lim_{n\to\infty} u_n x^{n+2} \leqslant \lim_{n\to\infty} \left(\frac{\alpha^n}{\sqrt{5}} + 1\right) x^{n+2} =$$
$$= \frac{x^2}{\sqrt{5}} \lim_{n\to\infty} (\alpha x)^n + \lim_{n\to\infty} x^{n+2}.$$

Comme $|\alpha x| < 1$, on a $|x| < 1$ de sorte que les deux limites ci-dessus sont nulles. Pour la même raison

$$\lim_{n\to\infty} u_{n+1} x^{n+1} = 0.$$

Donc, en passant à la limite dans la formule (1.24) pour n tendant vers l'infini, on obtient

$$s(x) = \lim_{n\to\infty} s_n(x) = \lim_{n\to\infty} \frac{x - u_n x^{n+2} - u_{n+1} x^{n+1}}{1 - x - x^2} =$$
$$= \frac{1}{1 - x - x^2} \left(x - \lim_{n\to\infty} u_n x^{n+2} - \lim_{n\to\infty} u_{n+1} x^{n+1}\right) = \frac{1}{1 - x - x^2}.$$

Le résultat trouvé peut s'écrire sous forme développée

$$u_1 x + u_2 x^2 + \ldots + u_n x^n + \ldots = \frac{x}{1 - x - x^2}. \qquad (1.28)$$

En attribuant à la variable x telle ou telle valeur, on obtiendra chaque fois une formule concrète. Par exemple, pour $x = \frac{1}{2}$ on aura

$$\frac{u_1}{2} + \frac{u_2}{2^2} + \ldots + \frac{u_n}{2^n} + \ldots = 2.$$

24. La formule (1.28) peut être obtenue par d'autres raisonnements.

Ecrivons

$$u_1 x + u_2 x^2 + \ldots + u_n x^n + \ldots = s(x) \qquad (1.29)$$

$\Big($sans oublier que l'expression de $s(x)$ n'a un sens que si $|x| < \frac{1}{\alpha}\Big)$ et multiplions les deux membres de cette égalité par x et x^2:

$$u_1 x^2 + u_2 x^3 + \ldots + u_n x^{n+1} + \ldots = x s(x), \quad (1.30)$$

$$u_1 x^3 + u_2 x^4 + \ldots + u_n x^{n+2} + \ldots = x^2 s(x). \quad (1.31)$$

En retranchant les égalités (1.30) et (1.31) de (1.29) et en réduisant les termes semblables, on obtient

$$u_1 x + (u_2 - u_1) x^2 + (u_3 - u_2 - u_1) x^3 +$$
$$+ (u_4 - u_3 - u_2) x^4 + \ldots + (u_n - u_{n-1} - u_{n-2}) x^n + \ldots =$$
$$= (1 - x - x^2) s(x).$$

Toutes les expressions entre parenthèses du premier membre sont évidemment nulles, et l'égalité devient

$$x = (1 - x - x^2) s(x),$$

d'où (1.28).

25. Jusqu'à présent chaque fois qu'on parlait du terme u_n de la suite de Fibonacci, son numéro n était supposé entier positif. Pourtant, la formule de récurrence fondamentale qui définit les termes de la suite peut prendre une autre forme :

$$u_{n-2} = u_n - u_{n-1}. \qquad (1.32)$$

Elle sert alors à exprimer les termes aux numéros plus petits par des termes aux numéros plus grands.

En posant successivement $n = 2, 1, 0, -1, \ldots$ dans (1.32), on peut calculer

$$u_0 = 0, \; u_{-1} = 1, \; u_{-2} = -1, \; u_{-3} = 2, \; \ldots;$$

d'une manière générale, on vérifie facilement (le lecteur est prié de s'en convaincre lui-même) que

$$u_{-n} = (-1)^{n+1} u_n. \qquad (1.33)$$

Cette expression simple d'un terme de la suite de Fibonacci dont le numéro est un entier quelconque permet de réduire tous les problèmes sur de tels termes à des problèmes sur les termes ordinaires aux numéros naturels.

Par exemple, pour calculer la somme de n premiers termes « à l'envers » de la suite de Fibonacci

$$u_{-1} + u_{-2} + \ldots + u_{-n},$$

il suffit de la récrire en conformité avec (1.33) :

$$u_1 - u_2 + \ldots + (-1)^{n-1} u_n$$

et de se rappeler la formule (1.6) :

$$u_{-1} + u_{-2} + \ldots + u_{-n} = (-1)^{n+1} u_{n-1} + 1 =$$
$$= -u_{-n+1} + 1.$$

Lorsqu'il s'applique aux termes de la suite de Fibonacci et est fondé sur la relation de récurrence fondamentale, le raisonnement par récurrence suivant le schéma « de n et

$n+1$ à $n+2$ » peut se faire, grâce à la relation (1.32), suivant le schéma « de n et $n-1$ à $n-2$ ». En particulier, on démontre sans difficulté la formule importante (1.8)

$$u_{n+m} = u_{n-1}u_m + u_n u_{m+1}$$

pour n et m entiers quelconques.

26. Les relations fondamentales pour α et β:

$$\alpha^{n+2} = \alpha^n + \alpha^{n+1},$$
$$\beta^{n+2} = \beta^n + \beta^{n+1},$$

sont valables non seulement pour des valeurs positives de n mais aussi pour n entier quelconque (ces égalités subsistent pour n fractionnaire, mais cette question n'est pas envisagée ici). On en déduit facilement que la formule de Binet

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

est vraie pour tout n entier.

Pour terminer, notons que le résultat du n° 17 peut être étendu (par récurrence « à l'envers ») aux valeurs négatives de n:

$$\alpha^{-n} = u_{-n}\alpha + u_{-n-1}. \qquad (1.34)$$

Cette égalité peut être récrite de la façon suivante:

$$(-1)^n \beta^n = (-1)^n u_n \frac{1}{\beta} + (-1)^n u_{n+1}$$

ou

$$\beta^{n+1} = u_{n+1}\beta + u_n.$$

De plus, l'égalité (1.34) peut être mise sous la forme

$$\alpha^{-n} = (-1)^{n-1}u_n\alpha + (-1)^n u_{n+1},$$

c'est-à-dire

$$(-1)^n \alpha^{-n} = u_{n+1} - u_n\alpha$$

ou encore

$$\frac{u_{n+1}}{u_n} - \alpha = (-1)^n \alpha^{-n} \frac{1}{u_n}. \qquad (1.35)$$

§ 2 PROPRIÉTÉS DE DIVISIBILITÉ DES NOMBRES DE FIBONACCI

1. Etudions maintenant quelques propriétés de divisibilité des termes de la suite de Fibonacci.

● THÉORÈME. *Si n est divisible par m, alors u_n est divisible par u_m.*

● DÉMONSTRATION. Soit n un nombre divisible par m, c.-à-d. $n = mk$. Démontrons le théorème par récurrence sur k.

Pour $k = 1$ on a $n = m$, de sorte que dans ce cas la divisibilité de u_n par u_m est évidente. Supposons que u_{mk} soit divisible par u_m et considérons le nombre $u_{m(k+1)}$. Comme $u_{m(k+1)} = u_{mk+m}$, en vertu de (1.8) on a

$$u_{m(k+1)} = u_{mk-1}u_m + u_{mk}u_{m+1}.$$

Le premier terme du second membre de cette égalité est manifestement divisible par u_m. En ce qui concerne le deuxième, il est divisible par u_{mk} et donc par u_m selon l'hypothèse de récurrence. Par conséquent, la somme de ces deux termes, c.-à-d. $u_{m(k+1)}$, est aussi divisible par u_m. Le théorème est démontré.

2. Soit un nombre quelconque m. S'il existe au moins un terme u_n divisible par m, le nombre de tels termes est aussi grand que l'on veut. A part u_n, ce sont, par exemple, u_{2n}, u_{3n}, u_{4n}, . . .

Il serait donc intéressant de savoir si pour tout nombre donné m on peut trouver au moins un terme de la suite de Fibonacci qui soit divisible par m. Il se trouve que cela est possible.

Soit $\overline{k}$ le reste de la division du nombre k par m. Considérons la suite des couples de tels restes obtenus en divisant les termes de la suite de Fibonacci par m:

$$\langle \overline{u}_1, \overline{u}_2 \rangle, \ \langle \overline{u}_2, \overline{u}_3 \rangle, \ \langle \overline{u}_3, \overline{u}_4 \rangle, \ \ldots, \ \langle \overline{u}_n, \overline{u}_{n+1} \rangle, \ \ldots \quad (2.1)$$

Si l'on convient de considérer deux couples $\langle a_1, b_1 \rangle$ et $\langle a_2, b_2 \rangle$ comme égaux pour $a_1 = a_2$ et $b_1 = b_2$, le nombre de tous les couples distincts de restes de la division par m est égal à m^2. Donc si l'on considère les $(m^2 + 1)$ premiers termes de la suite (2.1), parmi eux il y aura forcément des couples égaux.

Soit $\langle \overline{u}_k, \overline{u}_{k+1} \rangle$ le premier couple de la suite (2.1) qui se répète. Montrons que c'est le couple $\langle 1, 1 \rangle$. En effet, supposons le contraire, c.-à-d. que le premier couple qui se répète est $\langle \overline{u}_k, \overline{u}_{k+1} \rangle$ avec $k > 1$. Cherchons dans (2.1) un couple $\langle \overline{u}_l, \overline{u}_{l+1} \rangle$ $(l > k)$ égal à $\langle \overline{u}_k, \overline{u}_{k+1} \rangle$. Puisque $u_{l-1} = u_{l+1} - u_l$, $u_{k-1} = u_{k+1} - u_k$ et $\overline{u}_{l+1} = \overline{u}_{k+1}$, $\overline{u}_l = \overline{u}_k$, les restes de la division de u_{l-1} et u_{k-1} par m doivent être aussi égaux, c.-à-d. $\overline{u}_{l-1} = \overline{u}_{k-1}$. Il s'ensuit donc que $\langle \overline{u}_{k-1}, \overline{u}_k \rangle = \langle \overline{u}_{l-1}, \overline{u}_l \rangle$, et comme le couple $\langle \overline{u}_{k-1}, \overline{u}_k \rangle$ précède le couple $\langle \overline{u}_k, \overline{u}_{k+1} \rangle$, ce dernier n'est pas le *premier* couple qui se répète, ce qui contredit l'hypothèse. Par conséquent, la supposition $k > 1$ est fausse, d'où l'on déduit que $k = 1$.

Ainsi, $\langle 1, 1 \rangle$ est le premier couple de la suite (2.1) qui se répète. Supposons qu'il se répète à la t-ième place (d'après ce qui a été établi plus haut, on peut considérer t comme vérifiant la relation $1 < t < m^2 + 1$), c.-à-d.

$$\langle \overline{u}_t, \overline{u}_{t+1} \rangle = \langle 1, 1 \rangle.$$

Cela signifie que les restes de la division de u_t et u_{t+1} par m sont égaux à 1. Par suite, leur différence est divisible par m. Mais

$$u_{t+1} - u_t = u_{t-1},$$

de sorte que c'est le $(t - 1)$-ième terme de la suite de Fibonacci qui est divisible par m.

Ainsi, on vient de démontrer le théorème suivant.

● THÉORÈME. *Quel que soit le nombre entier m, parmi les* $(m^2 - 1)$ *premiers termes de la suite de Fibonacci il existe au moins un qui soit divisible par m.*

Notons que le théorème démontré n'indique pas *quel est précisément* le terme divisible par m. Il affirme seulement que le premier terme divisible par m n'est pas très grand. Nous reviendrons sur cette question un peu plus loin.

Du fait que $\langle 1, 1 \rangle$ est le premier couple de la suite (2.1) qui se répète il résulte qu'à partir de u_t la suite des restes se répète. Cela signifie qu'elle est périodique. Par exemple, pour $m = 4$ sa période est :

$$1, 1, 2, 3, 1, 0. \qquad (2.2)$$

Dans ce cas la longueur de la période est égale à 6. Ainsi, si le nombre n est de la forme $6k + 1$, $6k + 2$ ou $6k + 5$, le reste de la division de u_n par 4 est égal à 1, si n est de la forme $6k + 3$, ce reste est égal à 2 et si $n = 6k + 4$, il est 3.

3. La nature arithmétique des termes de la suite de Fibonacci, leurs diviseurs sont des questions d'un grand intérêt. Démontrons que, pour n composé et différent de 4, u_n est un nombre composé.

En effet, pour un tel n on peut écrire $n = n_1 n_2$ avec $1 < n_1 < n$, $1 < n_2 < n$ et $n_1 > 2$ ou bien $n_2 > 2$. Pour fixer les idées supposons $n_1 > 2$. Alors, d'après le théorème que l'on vient de démontrer, u_n est divisible par u_{n_1} et $1 < u_{n_1} < u_n$, ce qui signifie que u_n est un nombre composé.

4. Avant de continuer l'étude de la suite de Fibonacci rappelons au lecteur quelques premières notions de la théorie des nombres.

Décrivons d'abord le procédé de calcul du plus grand commun diviseur des nombres a et b.

Effectuons la division euclidienne de a par b. Soient q_0

le quotient et r_1 le reste de cette division. Il est évident que

$$a = bq_0 + r_1 \quad \text{et} \quad 0 \leqslant r_1 < b.$$

Remarquons que si $a < b$, on a $q_0 = 0$.

Divisons ensuite b par r_1 et désignons le quotient par q_1 et le reste par r_2. Il est clair que $b = r_1q_1 + r_2$ et $0 \leqslant r_2 < r_1$. Comme $r_1 < b$, on doit avoir $q_1 \neq 0$. En divisant r_1 par r_2, nous trouvons $q_2 \neq 0$ et r_3 tels que $r_1 = q_2r_2 + r_3$ et $0 \leqslant r_3 < r_2$. Continuons le procédé tant que c'est possible.

Tôt ou tard notre procédé s'interrompt, car les entiers positifs $r_1, r_2, r_3, \ldots$ sont tous distincts et chacun est inférieur à b. Donc, leur nombre ne dépasse pas b, et le procédé doit s'arrêter au b-ième pas au plus et il ne peut se terminer que si l'une des divisions successives est exacte, c.-à-d. si l'on obtient un reste nul par lequel on ne peut plus diviser.

Le procédé décrit ci-dessus porte le nom d'*algorithme d'Euclide*. Etant appliqué aux nombres a et b, il conduit à la suite d'égalités:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\ldots\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n. \end{aligned} \tag{2.3}$$

Considérons le dernier terme non nul de la suite $a, b, r_1, r_2, \ldots, r_n$. En général, c'est r_n, mais, en particulier, il est possible que ce soit b (pour uniformiser l'écriture on peut poser $b = r_0$). Il est évident que r_{n-1} est divisible par r_n. Considérons l'avant-dernière égalité de (2.3). Les deux termes de son deuxième membre étant divisibles par r_n, il en est de même de r_{n-2}. De la même manière on peut successivement établir (le raisonnement par récurrence!) que r_n divise $r_{n-3}, r_{n-4}, \ldots$ et, enfin, b et a. Ainsi, r_n est

un diviseur commun à a et b. Montrons que r_n est le plus grand commun diviseur de a et b. Pour cela il suffit de montrer que tout diviseur commun à a et b est un diviseur de r_n.

Soit d un diviseur commun quelconque de a et b. De la première égalité (2.3) on voit que d doit diviser r_1. Mais alors, en vertu de la deuxième égalité (2.3), d divise r_2. De la même façon (toujours le raisonnement par récurrence !) on démontre que d divise $r_3, \ldots, r_{n-1}$ et, enfin, r_n.

Ainsi, nous avons démontré qu'appliqué à deux nombres naturels a et b, l'algorithme d'Euclide conduit effectivement à leur plus grand commun diviseur. Par la suite nous allons désigner le plus grand commun diviseur de a et b par PGCD (a, b).

Il est évident que a est divisible par b si, et seulement si, le PGCD $(a, b) = b$.

En qualité d'exemple calculons PGCD $(u_{20}, u_{15}) =$ $=$ PGCD (6765, 610) :

$$6765 = 610 \cdot 11 + 55,$$
$$610 = 55 \cdot 11 + 5,$$
$$55 = 5 \cdot 11.$$

Donc,

$$\text{PGCD}\,(u_{20}, u_{15}) = 5 = u_5.$$

Le fait que le plus grand commun diviseur de deux termes de la suite de Fibonacci est de nouveau un terme de cette suite n'est pas un effet du hasard. Nous démontrerons plus bas qu'il en est toujours ainsi.

5. Un procédé analogue à l'algorithme d'Euclide est utilisé en géométrie pour trouver la commune mesure de deux segments commensurables. En effet, considérons deux segments : l'un de longueur a et l'autre de longueur b. Retranchons du premier segment le second autant de fois que cela est possible (il est clair que si $b > a$, cela n'est en général pas possible) et désignons la longueur du reste par r_1. Evidemment, $r_1 < b$. Retranchons maintenant du segment de longueur b le segment de longueur r_1 autant de fois que cela est possible et désignons le nouveau reste par r_2. En procédant de la même façon, nous obtiendrons

une suite de segments dont les longueurs décroissent. Jusqu'ici, comme on le voit, la ressemblance avec l'algorithme d'Euclide est complète.

Mais ensuite on constate une différence essentielle entre le procédé géométrique décrit et l'algorithme d'Euclide appliqué aux entiers naturels: la suite de segments restes de la soustraction peut ne pas s'arrêter, car il est possible que ce procédé de soustraction de segments puisse être continué indéfiniment. C'est évidemment le cas de l'incommensurabilité des segments initiaux.

Démontrons maintenant quelques propriétés simples du plus grand commun diviseur de deux nombres.

6. Le PGCD (a, bc) est divisible par le PGCD (a, b). En effet, b étant divisible par le PGCD (a, b), bc l'est aussi; a est divisible par le PGCD (a, b) de façon évidente. Donc, d'après ce qu'on a démontré au nº 4, le PGCD (a, bc) est lui aussi divisible par le PGCD (a, b).

7. PGCD (ac, bc) = PGCD $(a, b) \cdot c$.

● DÉMONSTRATION. Supposons que les égalités (2.3) décrivent le procédé de calcul du PGCD (a, b). Il est facile de vérifier qu'en multipliant les deux membres de chacune de ces égalités par c, on obtient une suite d'égalités correspondant à l'algorithme d'Euclide appliqué aux nombres ac et bc. Le dernier reste non nul est alors égal à $r_n c$, c.-à-d. au PGCD $(a, b) \cdot c$.

8. Si PGCD $(a, c) = 1$, alors PGCD (a, bc) = PGCD (a, b). En effet, d'après le nº 6, le PGCD (a, bc) est un diviseur du PGCD (ab, bc). Mais, d'après le nº 7,

$$\text{PGCD}\,(ab, bc) = \text{PGCD}\,(a, c) \cdot b = 1 \cdot b = b.$$

Donc, b est divisible par le PGCD (a, bc). D'autre part, le PGCD (a, bc) est un diviseur de a. Cela implique, en vertu du nº 4, que le PGCD (a, bc) divise aussi le PGCD (a, b). Et comme, d'après le nº 6, celui-ci divise à son tour le PGCD (a, bc), on obtient PGCD (a, b) = PGCD (a, bc).

Supposons que bc soit divisible par a. Cela signifie que PGCD $(a, bc) = a$. Si en outre PGCD $(a, c) = 1$, d'après ce qui précède, PGCD $(a, b) = a$, c.-à-d. que b est divisible par a.

Si p est un nombre premier, alors, quel que soit a, ou bien a est divisible par p, ou bien a et p sont premiers entre eux. Il en résulte d'après ce qui précède que si le produit de deux nombres est divisible par un nombre premier p, au moins l'un des facteurs est divisible par p. Cette proposition s'étend de façon évidente par récurrence au cas du produit d'un nombre quelconque de facteurs.

9. En qualité d'exemple, qui sera utile dans la suite, étudions quelques questions concernant la divisibilité des coefficients binomiaux.

● THÉORÈME. *Si p est un nombre premier, $k \neq 0$ et $k \neq p$, alors C_p^k est divisible par p.*

● DÉMONSTRATION. Conformément au n° 14, § 1,

$$C_p^k = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \ldots k}.$$

Comme en réalité cette fraction est égale à un nombre entier, son numérateur doit être divisible par le dénominateur. Or, chaque facteur du dénominateur est inférieur à p et donc non divisible par p. Par conséquent, comme p est premier, d'après ce qui précède, le produit de ces facteurs, c.-à-d. le dénominateur tout entier, n'est pas divisible par p. Cela signifie que le dénominateur de la fraction ci-dessus est premier avec p.

Considérons le numérateur de cette fraction comme le produit de deux nombres p et $(p-1)\ldots(p-k+1)$. Ce produit est divisible par le dénominateur. Comme ce dernier est premier avec p, c'est le deuxième facteur, c.-à-d. $(p-1)\ldots(p-k+1)$, qui est divisible par le dénominateur. Posons $(p-1)\ldots(p-k+1) = t \cdot 1 \cdot 2 \ldots k$. Alors $C_p^k = tp$, ce qu'il fallait démontrer.

10. Si c est divisible par b, alors PGCD $(a, b) =$ PGCD $(a + c, b)$.

● DÉMONSTRATION. Supposons que l'application de l'algorithme d'Euclide aux nombres a et b conduise au système

d'égalités (2.3). Appliquons cet algorithme aux nombres $a + c$ et b. Comme par hypothèse c est divisible par b, on peut poser $c = c_1 b$; le premier pas de l'algorithme nous donne l'égalité

$$a + c = (q_0 + c_1)\, b + r_1.$$

Les pas suivants donnent successivement la deuxième, la troisième égalité du système (2.3), etc. Le dernier reste non nul est toujours r_n, ce qui signifie que PGCD $(a, b) =$ $=$ PGCD $(a + c, b)$.

Le lecteur aura intérêt à démontrer ce théorème à l'aide de seuls résultats des nos 6-8, c.-à-d. sans recourir une deuxième fois à l'algorithme d'Euclide et au système (2.3).

11. THÉORÈME. *Tout terme de la suite de Fibonacci est premier avec son voisin.*

● DÉMONSTRATION. Supposons que contrairement à l'hypothèse u_n et u_{n+1} aient un diviseur commun $d > 1$. Alors leur différence $u_{n+1} - u_n$ est divisible par d. Mais comme $u_{n+1} - u_n = u_{n-1}$, u_{n-1} doit être lui aussi divisible par d. De manière analogue (raisonnement par récurrence!) on peut montrer que d est un diviseur de u_{n-2}, de u_{n-3}, etc., et, enfin, de u_1. Mais comme $u_1 = 1$, il ne peut pas être divisible par $d > 1$. La contradiction obtenue démontre le théorème.

12. THÉORÈME. PGCD $(u_m, u_n) = u_{(m,\, n)}$.

● DÉMONSTRATION. Pour fixer les idées supposons que $m > n$. En appliquant l'algorithme d'Euclide aux nombres m et n, on obtient :

$$\begin{aligned}
m &= nq_0 + r_1, & 0 &\leqslant r_1 < n,\\
n &= r_1 q_1 + r_2, & 0 &\leqslant r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, & 0 &\leqslant r_3 < r_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & &\\
r_{t-2} &= r_{t-1} q_{t-1} + r_t, & 0 &\leqslant r_t < r_{t-1},\\
r_{t-1} &= r_t q_t. & &
\end{aligned}$$

Comme on le sait, r_t est le plus grand commun diviseur de m et n.

Ainsi, $m = nq_0 + r_1$; cela signifie que

$$\text{PGCD}\,(u_m, u_n) = \text{PGCD}\,(u_{nq_0+r_1}, u_n),$$

ou

$$\text{PGCD}\,(u_m, u_n) = \text{PGCD}\,(u_{nq_0-1}u_{r_1} + u_{nq_0}u_{r_1+1}, u_n),$$

d'où, en vertu des nos 1 et 9,

$$\text{PGCD}\,(u_m, u_n) = \text{PGCD}\,(u_{nq_0-1}u_{r_1}, u_n),$$

ou, compte tenu des nos 11 et 8,

$$\text{PGCD}\,(u_m, u_n) = \text{PGCD}\,(u_{r_1}, u_n).$$

De manière analogue on peut démontrer que

$$\text{PGCD}\,(u_{r_1}, u_n) = \text{PGCD}\,(u_{r_2}, u_{r_1}),$$

$$\text{PGCD}\,(u_{r_2}, u_{r_1}) = \text{PGCD}\,(u_{r_3}, u_{r_2}),$$

. . . .

$$\text{PGCD}\,(u_{r_{t-1}}, u_{r_{t-2}}) = \text{PGCD}\,(u_{r_t}, u_{r_{t-1}}).$$

En comparant ces égalités, on voit que

$$\text{PGCD}\,(u_m, u_n) = \text{PGCD}\,(u_{r_t}, u_{r_{t-1}}),$$

et comme r_{t-1} est divisible par r_t, de sorte que $u_{r_{t-1}}$ est divisible par u_{r_t}, on doit avoir $(u_{r_t}, u_{r_{t-1}}) = u_{r_t}$. Enfin, si l'on remarque que $r_t = \text{PGCD}\,(m, n)$, on obtient le résultat cherché.

En particulier, il résulte du théorème que l'on vient de démontrer la réciproque de celui du n° 1 : si u_n est divisible par u_m, alors n est divisible par m. En effet, si u_n est divisible par u_m, alors, comme on l'a vu au n° 4,

$$\text{PGCD}\,(u_n, u_m) = u_m. \tag{2.4}$$

Or, d'après le théorème précédent

$$\text{PGCD}\,(u_n, u_m) = u_{(n,\,m)}. \qquad (2.5)$$

En comparant les formules (2.4) et (2.5), on obtient

$$u_m = u_{(n,\,m)},$$

c.-à-d. $m = \text{PGCD}\,(n, m)$, ce qui signifie que n est divisible par m.

13. En réunissant le théorème du nº 1 et la conséquence du théorème du nº 12, on obtient le résultat suivant: *u_n est divisible par u_m si, et seulement si, n est divisible par m.*

On en conclut qu'il est possible de juger de la divisibilité des termes de la suite de Fibonacci d'après la divisibilité de leurs numéros.

Etablissons quelques caractères de divisibilité des termes de la suite de Fibonacci en sous-entendant par le caractère un critère qui permet de trouver si tel ou tel terme est divisible par un nombre donné quelconque.

Un terme de la suite de Fibonacci est pair si, et seulement si, son numéro est divisible par 3.

Un terme de la suite de Fibonacci est divisible par 3 si, et seulement si, son numéro est divisible par 4.

Un terme de la suite de Fibonacci est divisible par 4 si, et seulement si, son numéro est divisible par 6.

Un terme de la suite de Fibonacci est divisible par 5 si, et seulement si, son numéro est divisible par 5.

Un terme de la suite de Fibonacci est divisible par 7 si, et seulement si, son numéro est divisible par 8.

La démonstration de ces caractères de divisibilité et de tous les autres du même genre peut être effectuée sans difficulté par le lecteur à l'aide de la proposition donnée au début de ce numéro et en considérant respectivement le troisième, le quatrième, le cinquième, le sixième, le huitième, etc., terme de la suite de Fibonacci.

On propose au lecteur de démontrer par la même occasion qu'il n'existe pas de termes de la suite de Fibonacci qui étant divisés par 8 donnent 4 pour reste, ni de termes impairs divisibles par 17.

14. Au cours de ce paragraphe nous aurons souvent à énoncer des propositions du type : « a et b divisés par m donnent le même reste », ou, ce qui revient au même, « la différence $a - b$ est divisible par m ».

Il faut que nous manipulions aisément ces propositions et passions sans difficulté aucune de telles propositions à telles autres. Nous emploierons donc, comme il est d'usage dans la théorie des nombres, l'écriture formelle, de sorte que les propositions deviennent l'objet d'un « calcul ».

● DÉFINITION. Les nombres a et b sont dits *congrus modulo m* si, en les divisant par m, on obtient le même reste ou si $a - b$ est divisible par m. La congruence modulo m de a et b se note

$$a \equiv b \pmod{m}.$$

Il est évident que si a est divisible par m, alors

$$a \equiv 0 \pmod{m}$$

et inversement.

15. Les congruences par rapport au même module peuvent être additionnées membre à membre comme les égalités.

● LEMME. *Si*

$$a_1 \equiv b_1 \pmod{m},$$
$$a_2 \equiv b_2 \pmod{m},$$
$$\dots\dots\dots$$
$$a_n \equiv b_n \pmod{m},$$

alors

$$a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod{m}.$$

● DÉMONSTRATION. De l'hypothèse il résulte que chacune des différences

$$a_1 - b_1,\ a_2 - b_2,\ \dots,\ a_n - b_n$$

est divisible par m ; donc, leur somme

$$(a_1 - b_1) + (a_2 - b_2) + \dots + (a_n - b_n),$$

ou

$$(a_1 + a_2 + \dots + a_n) - (b_1 + b_2 + \dots + b_n)$$

est aussi divisible par m, ce qui équivaut à la congruence demandée.

16. Au nº 9 nous avons démontré que pour p premier et $0 < k < p$ on a

$$C_p^k \equiv 0 \pmod p. \tag{2.6}$$

Cela peut s'écrire encore sous la forme

$$C_p^{k+1} \equiv 0 \pmod p \tag{2.7}$$

pour $0 \leqslant k < p - 1$.

Donc, pour $0 < k < p - 1$ les congruences (2.6) et (2.7) sont vraies toutes les deux. En les additionnant membre à membre, on obtient

$$C_p^k + C_p^{k+1} \equiv 0 \pmod p,$$

ou

$$C_{p+1}^{k+1} \equiv 0 \pmod p.$$

En d'autres termes, pour p premier tous les éléments de la $(p + 1)$-ième ligne du triangle de Pascal, excepté quatre (les deux extrêmes gauches et les deux extrêmes droits), sont divisibles par p.

Il est de même facile de vérifier que

$$C_{p+1}^0 \equiv C_{p+1}^1 \equiv C_{p+1}^p \equiv C_{p+1}^{p+1} \equiv 1 \pmod p.$$

17. La congruence (2.6) peut être récrite sous la forme

$$C_{p-1}^{k-1} + C_{p-1}^k \equiv 0 \pmod p,$$

ou

$$C_{p-1}^{k-1} \equiv -C_{p-1}^k \pmod p.$$

Elle est vraie pour $k = 1, 2, \ldots, p - 1$. Donc,

$$C_{p-1}^0 \equiv -C_{p-1}^1 \equiv C_{p-1}^2 \equiv -C_{p-1}^3 \equiv \ldots \equiv C_{p-1}^{p-1} \pmod p.$$

Comme $C_{p-1}^0 = 1$, la dernière congruence signifie que les éléments de la $(p - 1)$-ième ligne du triangle de Pascal sont congrus à 1 ou à -1 modulo p suivant que leurs numéros sont impairs ou pairs.

18. Les congruences par rapport au même module peuvent être non seulement additionnées, mais aussi multipliées membre à membre.

● LEMME. *Si*

$$\begin{aligned} a_1 &\equiv b_1 \pmod m, \\ a_2 &\equiv b_2 \pmod m, \\ &\cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ a_n &\equiv b_n \pmod m, \end{aligned} \tag{2.8}$$

alors

$$a_1a_2 \dots a_n \equiv b_1b_2 \dots b_n \pmod{m}. \qquad (2.9)$$

● DÉMONSTRATION. On va démontrer ce lemme par récurrence sur n.

Pour $n = 1$ il est évident.

Supposons que le lemme soit vrai pour une valeur quelconque de n (c.-à-d. que (2.8) implique (2.9)) et complétons ses hypothèses par la congruence

$$a_{n+1} \equiv b_{n+1} \pmod{m}. \qquad (2.10)$$

Les congruences (2.9) et (2.10) signifient respectivement que $a_1a_2 \dots a_n - b_1b_2 \dots b_n$ et $a_{n+1} - b_{n+1}$ sont divisibles par m. Par conséquent,

$$a_1a_2 \dots a_n = b_1b_2 \dots b_n + mT,$$
$$a_{n+1} = b_{n+1} + mt,$$

où T et t sont des nombres entiers. En multipliant membre à membre ces égalités on obtient

$$a_1a_2 \dots a_na_{n+1} = b_1b_2 \dots b_nb_{n+1} + \\ + m(b_1b_2 \dots b_nt + b_{n+1}T + mTt).$$

Les parenthèses du deuxième membre contiennent un nombre entier; donc,

$$a_1a_2 \dots a_na_{n+1} \equiv b_1b_2 \dots b_nb_{n+1} \pmod{m},$$

ce qu'il fallait démontrer.

Du lemme démontré il résulte qu'on peut élever les deux membres d'une congruence à toute puissance entière non négative.

Un cas particulier trivial du lemme précédent est exprimé par le fait suivant: le produit de plusieurs nombres de la forme $4t + 1$ est lui aussi un nombre de la forme $4t + 1$. En effet, soient $a_1, a_2, \dots, a_n$ les nombres donnés.

Par hypothèse

$$a_1 \equiv 1 \pmod{4},\ a_2 \equiv 1 \pmod{4},\ \dots,\ a_n \equiv 1 \pmod{4}.$$

En multipliant membre à membre ces congruences on obtient

$$a_1a_2 \dots a_n \equiv 1 \pmod{4}.$$

19. Les règles de simplification des congruences sont semblables aux règles de simplification des égalités: une égalité peut être simplifiée par tout nombre non nul et une congruence par tout nombre premier avec le module.

● LEMME. *Si*

$$ac \equiv bc \pmod{m} \qquad (2.11)$$

et PGCD $(c, m) = 1$, *alors*

$$a \equiv b \pmod{m}. \qquad (2.12)$$

● DÉMONSTRATION. La congruence (2.11) signifie que la différence $ac - bc$ est divisible par m. Mais

$$ac - bc = (a - b)\, c,$$

et comme PGCD$(c, m) = 1$, c'est la différence $a - b$ qui est divisible par m, ce qui équivaut à la congruence (2.12).

20. La proposition suivante, appelée théorème de Fermat, s'avère utile dans de nombreuses questions.

● THÉORÈME. *Si p est un nombre premier et a n'est pas divisible par p, alors*

$$a^{p-1} \equiv 1 \pmod{p}.$$

● DÉMONSTRATION. Considérons les nombres

$$a,\ 2a,\ \ldots,\ (p - 1)a. \qquad (2.13)$$

Ils ne sont pas congrus modulo p deux à deux. En effet, comme PGCD $(a, p) = 1$, la congruence

$$ka \equiv la \pmod{p}$$

m pliquerait, d'après le lemme du n° 19, que

$$k \equiv l \pmod{p},$$

c.-à-d. que $k - l$ est divisible par p, ce qui est impossible pour $0 < k$, $l < p$ et $k \neq l$.

En outre, aucun des nombres considérés n'est divisible par p.

Donc, la division des nombres (2.13) par p donne les restes r_1, $r_2, \ldots, r_{p-1}$, tous distincts et non nuls. Ainsi, nous avons $(p - 1)$ nombres (2.13), de même que $(p - 1)$ restes distincts non nuls de leur division par p. Par conséquent, parmi les restes de la division des nombres (2.13) par p (c.-à-d. parmi les nombres $r_1, r_2, \ldots, \ldots, r_{p-1}$), chacun des restes $1, 2, \ldots, p - 1$ figure exactement une fois. On a donc

$$a \equiv r_1 \pmod{p},$$
$$2a \equiv r_2 \pmod{p},$$
$$\cdots\cdots$$
$$(p - 1)\, a \equiv r_{p-1} \pmod{p}.$$

En multipliant ces congruences membre à membre, on obtient

$$1 \cdot 2 \ldots (p - 1)\, a^{p-1} \equiv r_1 r_2 \ldots r_{p-1} \pmod{p}. \qquad (2.14)$$

Or, comme nous l'avons déjà noté, les nombres $r_1, r_2, \ldots, r_{p-1}$

ne sont rien d'autre que 1, 2, . . ., $p - 1$, seulement écrits dans un ordre différent. Donc, la congruence (2.14) peut être récrite sous la forme

$$1 \cdot 2 \dots (p-1)\, a^{p-1} \equiv 1 \cdot 2 \dots (p-1) \pmod p. \qquad (2.15)$$

Remarquons enfin que le produit $1 \cdot 2 \dots (p-1)$ est premier avec p; donc, la congruence (2.15) peut être simplifiée:

$$a^{p-1} \equiv 1 \pmod p,$$

ce qu'il fallait démontrer.

21. Du nº 2 il résulte que parmi les diviseurs des termes de la suite de Fibonacci on peut trouver en général n importe quel nombre. Nous allons voir maintenant qu'on peut distinguer certaines classes de ces termes admettant des diviseurs d'une forme assez concrète.

On a, par exemple, le théorème suivant:

● THÉORÈME. *Si un terme de la suite de Fibonacci a le numéro impair, tous ses diviseurs impairs sont de la forme* $4t + 1$.

● DÉMONSTRATION. La formule (1.10) (v. nº 9, § 1) donne pour n impair

$$u_n^2 = u_{n-1}u_{n+1} + 1,$$

d'où

$$u_{n-1}u_{n+1} - u_n^2 = u_{n-1}(u_{n-1} + u_n) - u_n^2 =$$
$$= u_{n-1}^2 + u_{n-1}u_n - u_n^2 = -1. \qquad (2.16)$$

Soit p un diviseur premier de u_n et $p \neq 2$. De (2.16) on voit que $u_{n-1}^2 + 1$ est divisible par u_n, donc par p aussi. Par conséquent,

$$u_{n-1}^2 \equiv -1 \pmod p.$$

En élevant les deux membres de cette congruence à la puissance $\frac{p-1}{2}$, on obtient:

$$(u_{n-1}^2)^{\frac{p-1}{2}} = u_{n-1}^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

D'autre part, PGCD$(u_{n-1}, u_n) = 1$, de sorte que u_{n-1} n'est pas divisible par p et on retrouve les conditions du théorème de Fermat énoncé ci-dessus, d'après lequel on a

$$u_{n-1}^{p-1} \equiv 1 \pmod p.$$

Mais alors on a également

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p,$$

c.-à-d. $(-1)^{\frac{p-1}{2}} = 1$. Par conséquent, le nombre $\frac{p-1}{2}$ est pair, ce qui signifie que p est de la forme $4t+1$.

Ainsi, tous les diviseurs impairs premiers de u_n sont de la forme $4t+1$. Donc, d'après ce qui a été dit à la fin du nº 18, c'est également celle de tout produit de tels diviseurs, c'est-à-dire de tout diviseur impair de u_n (v. nº 5, § 1).

22. D'après la définition de la congruence, tous les nombres qui, étant divisés par m, donnent le même reste sont congrus modulo m. Par contre, si les restes obtenus sont différents, les nombres donnés ne le sont pas.

Le reste de la division par m ne peut être que l'un des m nombres: $0, 1, 2, \ldots, m-1$. Donc, il ne peut y avoir que m nombres non congrus modulo m.

Soit m impair; considérons les nombres

$$-\frac{m-1}{2},\ -\frac{m-3}{2},\ \ldots,\ -1,\ 0,\ 1,\ 2,\ \ldots,\ \frac{m-3}{2},\ \frac{m-1}{2}. \quad (2.17)$$

Ils sont m et n'importe quels deux nombres de cette suite ne sont congrus modulo m (sinon leur différence, qui est non nulle et est inférieure à m en valeur absolue, serait divisible par m). Par conséquent, tout nombre est congru à l'un des nombres (2.17) modulo m. Les nombres (2.17) sont appelés *les plus petits résidus modulo m*. Il est évident que chacun d'eux est en valeur absolue inférieur à la moitié du module m.

Remarquons que le système des plus petits résidus modulo m peut être construit aussi pour m pair. Il est un peu différent de (2.17):

$$-\frac{m-2}{2},\ -\frac{m-4}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-2}{2},\ \frac{m}{2}.$$

Nous n'aurons d'ailleurs pas besoin de ce système.

23. Soit m un entier impair non divisible par 5. Construisons la suite des plus petits résidus modulo m des nombres $5, 2\cdot5, 3\cdot5, \ldots, \frac{m-1}{2}\cdot5$.

Par exemple, pour $m = 21$ cette suite est

$$5,\ 10,\ -6,\ -1,\ 4,\ 9,\ -7,\ -2,\ 3,\ 8.$$

Examinons l'alternance des signes dans les suites de ce type pour des valeurs diverses de m. Il se trouve qu'elle dépend du dernier chiffre de m (écrit en numération décimale).

● LEMME. *Si $m = 10t+1$, la suite des plus petits résidus est construite de la manière suivante:*

t termes positifs, t termes négatifs, t termes positifs, t termes négatifs, t termes positifs.

Si $m = 10t + 3$, *le schéma d'alternance des signes est le suivant:*

t termes positifs, t termes négatifs, t termes positifs, $(t + 1)$ *termes négatifs, t termes positifs.*

Si $m = 10t + 7$, *les termes de la suite sont rangés comme suit:*

t termes positifs, $(t + 1)$ *termes négatifs,* $(t + 1)$ *termes positifs, t termes négatifs,* $(t + 1)$ *termes positifs.*

Si $m = 10t + 9$, *on a t termes positifs,* $(t + 1)$ *termes négatifs,* $(t + 1)$ *termes positifs,* $(t + 1)$ *termes négatifs,* $(t + 1)$ *termes positifs.*

La démonstration se fait par calcul direct de chacune des quatre propositions ci-dessus prises séparément. Nous nous bornons à la démonstration de la première, en laissant celle des autres propositions au soin du lecteur.

Ainsi, soit $m = 10t + 1$. Il est évident que pour $k \leqslant t$ on a $5k < \frac{m-1}{2}$, de sorte que tous les nombres de la forme $5k$ sont les plus petits résidus modulo m. Ils sont au nombre de t et le dernier est $5t$. Comme $5(t + 1) > \frac{m-1}{2}$, le terme suivant de la suite cherchée est négatif (il est égal à $-5t + 4$). En lui ajoutant successivement $(t - 1)$ fois le nombre 5, on obtient une série de t nombres négatifs dont le dernier est -1. Vient ensuite le nombre positif 4, suivi de $(t - 1)$ autres nombres positifs (c.-à-d. jusqu'à $4 + (t - 1)\cdot 5 = 5t - 1$ inclusivement), après quoi on tombe de nouveau sur des nombres négatifs (de $-5t + 3$ à -2; en tout t nombres). Enfin, on obtient encore t nombres positifs (de 3 à $5t - 2$) qui achèvent la suite. La première proposition est démontrée.

En fait, ce qui est particulièrement important pour nous dans ce lemme, c'est que la suite des plus petits résidus modulo m contient pour $m = 10t \pm 1$ un nombre pair de termes négatifs et un nombre impair pour $m = 10t \pm 3$.

24. LEMME. *Si p est un nombre premier de la forme* $5t \pm 1$, *alors* $5^{\frac{p-1}{2}} - 1$ *est divisible par p.*

Si p est un nombre premier de la forme $5t \pm 2$, *alors* $5^{\frac{p-1}{2}} + 1$ *est divisible par p.*

● **DÉMONSTRATION.** On a

$$5 \equiv \varepsilon_1 r_1 \pmod{p},$$
$$2\cdot 5 \equiv \varepsilon_2 r_2 \pmod{p},$$
$$\cdots\cdots\cdots\cdots$$
$$\frac{p-1}{2}\cdot 5 \equiv \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}} \pmod{p},$$

où $\varepsilon_k r_k$ est le plus petit résidu du nombre $k\cdot 5$ par rapport au module p, $r_k > 0$, et $\varepsilon_k = \pm 1$, ce qui définit le signe du résidu.

En multipliant ces congruences membre à membre, on obtient

$$1\cdot 2 \ldots \frac{p-1}{2} \cdot 5^{\frac{p-1}{2}} \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}} r_1 r_2 \ldots r_{\frac{p-1}{2}} \pmod p. \qquad (2.18)$$

On raisonne ensuite de manière analogue à celle de la démonstration du théorème de Fermat.

Chacun des nombres positifs $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ est inférieur ou égal à $\frac{p-1}{2}$.

Si parmi ces nombres il y avait deux égaux: $r_k = r_l$ $\left(1 \leqslant k, l \leqslant \frac{p-1}{2}\right)$, on aurait $5k \equiv \pm 5l \pmod p$ ou, puisque PGCD$(5, p) = 1$, $k \equiv \pm l \pmod p$. Or, cela est impossible, car $-p < k - l < k + l < p$ et $k - l \neq 0$. Par conséquent, tous les nombres $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ sont distincts. Ils coïncident donc à l'ordre près avec les nombres $1, 2, \ldots, \frac{p-1}{2}$. Comme ils sont tous premiers avec le module, on peut simplifier la congruence (2.18) par le produit $1\cdot 2 \ldots \frac{p-1}{2}$. On obtient alors

$$5^{\frac{p-1}{2}} \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}} \pmod p.$$

D'après le lemme du n° 23, le nombre de facteurs égaux à -1 dans le produit $\varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}}$ est pair, si $p = 10t \pm 1$ (puisque p est impair, cela est équivalent à ce que p soit de la forme $5t \pm 1$), et impair, si $p = 10t \pm 3$ (c.-à-d. si p est de la forme $5t \pm 2$).

De là on déduit immédiatement les deux affirmations du lemme.

25. Maintenant nous pouvons démontrer la propriété fondamentale de la divisibilité des termes de la suite de Fibonacci par un nombre premier.

● THÉORÈME. *Si le nombre premier p est de la forme* $5t \pm 1$, *alors* u_{p-1} *est divisible par p. Si p est de la forme* $5t \pm 2$, *alors* u_{p+1} *est divisible par p.*

● DÉMONSTRATION. Supposons que p soit de la forme $5t \pm \pm 1$. D'après la formule de Binet, on a

$$u_{p-1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{p-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p-1}\right) =$$

$$= \frac{1}{\sqrt{5}}\,\frac{1}{2^{p-1}}\left(1 + C_{p-1}^{1}\sqrt{5} + C_{p-1}^{2}(\sqrt{5})^2 + \ldots + C_{p-1}^{p-1}(\sqrt{5})^{p-1} -\right.$$

$$\left. - 1 + C_{p-1}^{1}\sqrt{5} - C_{p-1}^{2}(\sqrt{5})^2 + \ldots - C_{p-1}^{p-1}(\sqrt{5})^{p-1}\right),$$

ou, après des simplifications évidentes,

$$u_{p-1} = \frac{1}{2^{p-2}}\left(C_{p-1}^{1} + C_{p-1}^{3}\cdot 5 + C_{p-1}^{5}\cdot 5^2 + \ldots + C_{p-1}^{p-2}\cdot 5^{\frac{p-3}{2}}\right).$$

En vertu du nº 17 tous les coefficients binomiaux énumérés ici sont congrus à 1 modulo p. Par suite,

$$2^{p-1}u_{p-1} \equiv 2\left(1 + 5 + \ldots + 5^{\frac{p-3}{2}}\right) \pmod{p}.$$

Calculant la somme de la progression géométrique ci-dessus et prenant en considération que 2^{p-1} est congru à 1 modulo p, on obtient

$$u_{p-1} \equiv \frac{5^{\frac{p-1}{2}} - 1}{2} \pmod{p}.$$

Or, d'après ce qui précède, le numérateur de la fraction du deuxième membre est divisible par p. Comme PGCD $(p, 2) = 1$, il en est de même de la fraction toute entière. Par conséquent, u_{p-1} est divisible par p, de sorte que la première partie du théorème est démontrée.

Considérons maintenant le cas où p est de la forme $5t \pm 2$. En appliquant comme plus haut la formule de Binet, on obtient

$$u_{p+1} = \frac{1}{2^p}\left(C_{p+1}^{1} + C_{p+1}^{3}\cdot 5 + C_{p+1}^{5}\cdot 5^2 + \ldots + C_{p+1}^{p}\cdot 5^{\frac{p-1}{2}}\right) \pmod{p}.$$

D'après le nº 16 tous les termes entre parenthèses, sauf les deux extrêmes, sont divisibles par p, et $C_{p+1}^{1} = C_{p+1}^{p}$ divisé par p donne 1 pour reste. Par suite,

$$u_{p+1} \equiv \frac{1}{2}\left(1 + 5^{\frac{p-1}{2}}\right) \pmod{p}.$$

En appliquant le lemme précédent, on déduit dans ce cas que u_{p+1} est divisible par p.

26. Supposons que u_n soit divisible par un nombre premier quelconque p et que tous les termes de la suite de Fibonacci inférieurs à u_n soient non divisibles par p. Dans ce cas on dit que p est *diviseur propre* de u_n. Par exemple, 11 est diviseur propre de u_{10}, 17 est diviseur propre de u_9, etc.

Tout terme de la suite de Fibonacci, sauf u_1, u_2, u_6 et u_{12}, possède au moins un diviseur propre.

La démonstration de ce fait appelle des raisonnements assez compliqués et nous occupera jusqu'à la fin de ce paragraphe. Ce faisant, nous établirons d'autres propriétés des termes de la suite de Fibonacci concernant leur divisibilité.

27. Commençons par quelques considérations d'ordre général.

Le résultat sur la divisibilité d'un produit par un nombre premier, établi au nº 8, permet de démontrer le théorème que l'on appelle souvent « théorème fondamental de l'arithmétique ».

● THÉORÈME. *Tout entier naturel est décomposable en facteurs premiers de manière unique.*

● DÉMONSTRATION. Remarquons tout d'abord que la possibilité d'une telle décomposition est un fait très simple qui a été déjà établi de façon directe au nº 5 du § 1 à l'aide d'un raisonnement par récurrence.

Pour démontrer l'unicité considérons deux décompositions possibles du nombre a en facteurs premiers:

$$p_1p_2 \ldots p_k = a = q_1q_2 \ldots q_l.$$

Pour fixer les idées, supposons que $k \leqslant l$. Le deuxième membre de l'égalité ci-dessus doit être divisible par p_1. Donc, en vertu du nº 8, au moins l'un des facteurs qu'il contient doit être divisible par p_1. Soit q_1 ce facteur. Comme q_1 est un nombre premier, cela n'est possible que si $p_1 = q_1$. En simplifiant on trouve

$$p_2 \ldots p_k = q_2 \ldots q_l.$$

En répétant le même raisonnement k fois (démonstration par récurrence !), c.-à-d. jusqu'à l'épuisement de tous les facteurs du premier membre, on obtient finalement

$$1 = q_{k+1} \ldots q_l.$$

Mais cette dernière égalité peut avoir lieu seulement pour $q_{k+1} = \ldots$ $\ldots = q_l = 1$, ce qui veut dire que les facteurs premiers $q_{k+1}, \ldots$ $\ldots, q_l$ doivent manquer.

Le théorème est démontré.

28. Les facteurs égaux de la décomposition du nombre a en facteurs premiers étant groupés en puissances, on peut écrire

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}. \tag{2.19}$$

Cette représentation de l'entier naturel a est sa *décomposition canonique.*

Parfois, pour des raisons de commodité, nous allons ajouter à la décomposition canonique d'un nombre de nouveaux facteurs premiers munis des exposants nuls.

29. Evidemment, pour que le nombre a de décomposition canonique (2.19) soit divisible par

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \tag{2.20}$$

il faut et il suffit que l'on ait

$$\beta_1 \leqslant \alpha_1, \ \beta_2 \leqslant \alpha_2, \ \dots, \ \beta_k \leqslant \alpha_k.$$

(En particulier, si pour i quelconque $\alpha_i = 0$, on doit avoir aussi $\beta_i = 0$.)

Maintenant nous pouvons décrire d'une façon nouvelle le plus grand commun diviseur de deux ou plusieurs nombres.

Soient $a_1, a_2, \dots, a_n$ n nombres naturels quelconques et $p_1, \dots$ $\dots, p_k$ les nombres premiers dont chacun divise au moins l'un de ces nombres. Ecrivons les décompositions canoniques de $a_1, a_2, \dots$ $\dots, a_n$:

$$\begin{aligned} a_1 &= p_1^{\alpha_{11}} p_2^{\alpha_{12}} \dots p_k^{\alpha_{1k}}, \\ a_2 &= p_1^{\alpha_{21}} p_2^{\alpha_{22}} \dots p_k^{\alpha_{2k}}, \\ &\dots\dots\dots\dots \\ a_n &= p_1^{\alpha_{n1}} p_2^{\alpha_{n2}} \dots p_k^{\alpha_{nk}} \end{aligned} \tag{2.21}$$

(ici tous les exposants $\alpha_{ij} \geqslant 0$). Il est clair que la décomposition canonique de tout diviseur commun d des nombres $a_1, \dots, a_n$ ne peut contenir que des facteurs premiers, pris parmi les nombres $p_1, \dots, p_k$:

$$d = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}.$$

Ici chaque exposant δ_i doit être inférieur ou égal à chacun des exposants correspondants $\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}$ du nombre p_i dans les décompositions canoniques de $a_1, a_2, \ldots, a_n$:

$$\delta_i \leqslant \alpha_{1i}, \ \delta_i \leqslant \alpha_{2i}, \ \ldots, \ \delta_i \leqslant \alpha_{ni}. \qquad (2.22)$$

Si α est *le plus grand* commun diviseur, les exposants δ_i sont les plus grands des nombres qui vérifient les inégalités correspondantes (2.22). Mais cela signifie que chaque δ_i est tout simplement le plus petit des nombres $\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}$. On peut écrire:

$$\delta_i = \min \{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}\}.$$

On désigne le plus grand commun diviseur des nombres $a_1, a_2, \ldots, a_n$, comme dans le cas de deux nombres, par PGCD $(a_1, a_2, \ldots, a_n)$.

30. Une notion en quelque sorte duale de celle de plus grand commun diviseur est la notion de plus petit commun multiple.

Il est évident que la décomposition canonique de tout nombre divisible par les entiers $a_1, a_2, \ldots, a_n$ de décompositions canoniques (2.21) doit contenir tous les facteurs premiers figurant au moins une fois dans les décompositions (2.21), c.-à-d. les nombres $p_1, p_2, \ldots, p_k$. La décomposition canonique d'un multiple commun peut contenir encore des facteurs « étrangers ». Ainsi, la décomposition canonique de tout multiple commun m des nombres $a_1, a_2, \ldots, a_n$ doit être de la forme

$$m = p_1^{\mu_1} p_2^{\mu_2} \ldots p_k^{\mu_k} Q,$$

où Q désigne le produit de tous les facteurs premiers « étrangers ». De même, il est évident que pour tout $i = 1, \ldots, k$ on doit avoir

$$\mu_i \geqslant \alpha_{1i}, \ \mu_i \geqslant \alpha_{2i}, \ \ldots, \ \mu_i \geqslant \alpha_{ni}. \qquad (2.23)$$

Si m est *le plus petit* commun multiple des nombres $a_1, a_2, \ldots, a_n$, le facteur Q doit évidemment manquer (c.-à-d. qu'il doit être égal à 1), et les exposants μ_i doivent être les plus petits des exposants vérifiant les inégalités (2.23). Mais cela signifie que chaque μ_i doit être tout simplement le plus grand des nombres $\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}$:

$$\mu_i = \max \{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}\}.$$

Le plus petit commun multiple des nombres $a_1, a_2, \ldots, a_n$ est désigné par PPCM $(a_1, a_2, \ldots, a_n)$.

31. Démontrons le lemme auxiliaire suivant.

● LEMME. *Quels que soient les nombres* $\alpha_1, \alpha_2, \ldots, \alpha_n$, *on a*

$$\max\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \alpha_1 + \alpha_2 + \ldots + \alpha_n -$$
$$- \min\{\alpha_1, \alpha_2\} - \min\{\alpha_1, \alpha_3\} - \ldots - \min\{\alpha_{n-1}, \alpha_n\} +$$
$$+ \min\{\alpha_1, \alpha_2, \alpha_3\} + \min\{\alpha_1, \alpha_2, \alpha_4\} + \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (2.24)$$
$$\pm \min\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

(la deuxième ligne contient tous les minimums de deux nombres, la troisième tous les minimums de trois nombres, etc.).

● DÉMONSTRATION. Sans restreindre la généralité, on peut considérer dès le début les nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ comme disposés dans l'ordre de non-croissance:

$$\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_n.$$

Dans ce cas

$$\max\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \alpha_1.$$

Calculons la valeur du second membre de (2.24). Pour cela comptons combien de fois (algébriquement) y figure chacun des nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$. Dans le cas où deux nombres α_i et α_j sont égaux, nous allons considérer comme minimal celui qui a le plus grand numéro (évidemment, cette convention purement formelle n'exerce aucune influence sur les valeurs des expressions considérées).

Remarquons d'abord que α_1 est le plus grand des nombres considérés. C'est pourquoi il ne se trouve que dans la première ligne du second membre de (2.24), et cela une seule fois. Donc, le coefficient de α_1 dans le deuxième membre de (2.24) est égal à 1.

Examinons maintenant la façon dont un nombre quelconque α_i ($i > 1$) entre dans le second membre de (2.24). Il n'entre qu'une fois dans la première ligne. La deuxième ligne et les lignes suivantes, jusqu'à la i-ième inclusivement, le renferment seulement comme minimum qui est une combinaison de α_i avec des nombres de numéros inférieurs à i. α_i entrera donc dans la j-ième ligne ($j \leqslant i$) un nombre de fois égal au nombre des combinaisons de $i-1$ éléments $\alpha_1, \ldots, \alpha_{i-1}$ $j-1$ à $j-1$, c.-à-d. à C_{i-1}^{j-1} (v. nº 14, § 1). Ainsi, le second membre de (2.24) renfermera

$$1 - C_{i-1}^{1} + C_{i-1}^{2} - \ldots \pm C_{i-1}^{j-1}$$

α_i.

En vertu du nº 13, § 1 cette expression est égale à 0.

Par conséquent, le second membre de (2.24) est égal à α_1, c.-à-d. au premier membre, et le lemme est démontré.

32. Usons de ce qu'on vient de démontrer pour donner une description commode du plus petit commun multiple de plusieurs nombres.

● THÉORÈME.

$$\text{PPCM}(a_1, a_2, \ldots, a_n) =$$
$$= \frac{a_1a_2\ldots a_n \cdot \text{PGCD}(a_1, a_2, a_3)\cdot \text{PGCD}(a_1, a_2, a_4)\ldots}{\text{PGCD}(a_1, a_2)\cdot \text{PGCD}(a_1, a_3)\ldots \text{PGCD}(a_{n-1}, a_n)\,\text{PGCD}(a_1, a_2, a_3, a_4)\ldots}. \quad (2.25)$$

(Le numérateur de cette fraction représente le produit des nombres donnés et de tous les plus grands communs diviseurs de ces nombres, pris 3 à 3, 5 à 5, etc., et le dénominateur le produit de tous les plus grands communs diviseurs de ces nombres, pris 2 à 2, 4 à 4, etc.)

● DÉMONSTRATION. Soit p un facteur premier quelconque figurant dans les décompositions canoniques de quelques-uns des nombres $a_1, a_2, \ldots, a_n$. Désignons par α_i l'exposant de p dans la décomposition canonique de a_i. Alors, en vertu du nº 30, p entre dans le premier membre de (2.25) avec l'exposant

$$\max\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \quad (2.26)$$

et, d'après le nº 29, avec l'exposant

$$\begin{aligned}&\alpha_1 + \alpha_2 + \ldots + \alpha_n -\\ &- \min\{\alpha_1, \alpha_2\} - \min\{\alpha_1, \alpha_3\} - \ldots - \min\{\alpha_{n-1}, \alpha_n\} +\\ &+ \min\{\alpha_1, \alpha_2, \alpha_3\} + \min\{\alpha_1, \alpha_2, \alpha_4\} + \ldots\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ &\pm \min\{\alpha_1, \alpha_2, \ldots, \alpha_n\}\end{aligned} \quad (2.27)$$

dans le second membre. Mais d'après le lemme précédent les expressions (2.26) et (2.27) sont égales.

Ainsi, les décompositions canoniques du premier et du second membre de (2.25) renferment les mêmes facteurs premiers pris avec les mêmes exposants.

33. Reprenons maintenant l'étude de la divisibilité des termes de la suite de Fibonacci.

● LEMME.

$$u_{mn-1} - u_{n-1}^m \text{ est divisible par } u_n^2. \quad (2.28)$$

● DÉMONSTRATION. On démontre par récurrence sur m.

Pour $m = 1$ le dividende s'annule; donc, il est divisible par u_n^2. Supposons maintenant que (2.28) soit vraie pour m quelconque et considérons l'expression

$$u_{(m+1)n-1} - u_{n-1}^{m+1} = (u_{mn-1}u_{n-1} + u_{mn}u_n) - u_{n-1}^{m+1}.$$

D'après l'hypothèse de récurrence

$$u_{mn-1} \equiv u_{n-1}^m \pmod{u_n^2}.$$

Par suite,

$$u_{(m+1)n-1} - u_{n-1}^{m+1} \equiv u_{n-1}^{m} u_{n-1} + u_{mn} u_n - u_{n-1}^{m+1} \pmod{u_n^2}. \tag{2.29}$$

Du n° 1 il résulte que u_{mn} est divisible par u_n ; donc,

$$u_{mn} u_n \equiv 0 \pmod{u_n^2},$$

et (2.29) prend la forme

$$u_{(m+1)n-1} - u_{n-1}^{m+1} \equiv 0 \pmod{u_n^2}.$$

Le raisonnement par récurrence est terminé, et le théorème démontré.

34. LEMME.

$$u_{mn} - u_{n+1}^{m} + u_{n-1}^{m} \textit{ est divisible par } u_n^2. \tag{2.30}$$

● DÉMONSTRATION. On démontre par récurrence sur m.

Pour $m = 1$, le dividende s'annule ; donc, il est divisible par u_n^2.

Supposons que (2.30) ait lieu pour m quelconque et considérons l'expression

$$u_{(m+1)n} - u_{n+1}^{m+1} + u_{n-1}^{m+1} = u_{mn-1} u_n + u_{mn} u_{n+1} - u_{n+1}^{m+1} + u_{n-1}^{m+1}.$$

Or, selon l'hypothèse de récurrence,

$$u_{mn} \equiv u_{n+1}^{m} - u_{n-1}^{m} \pmod{u_n^2}.$$

Par conséquent,

$$u_{(m+1)n} - u_{n+1}^{m+1} + u_{n-1}^{m+1} \equiv u_{mn-1} u_n + u_{n+1}(u_{n+1}^{m} - u_{n-1}^{m}) - u_{n+1}^{m+1} + u_{n-1}^{m+1} \pmod{u_n^2},$$

ou

$$u_{(m+1)n} - u_{n+1}^{m+1} + u_{n-1}^{m+1} \equiv u_{mn-1} u_n - u_{n-1}^{m}(u_{n+1} - u_{n-1}) \pmod{u_n^2},$$

ou encore

$$u_{(m+1)n} - u_{n+1}^{m+1} + u_{n-1}^{m+1} \equiv u_n (u_{mn-1} - u_{n-1}^{m}) \pmod{u_n^2}.$$

D'après ce qui précède, la différence du deuxième membre est divisible par u_n^2. Par conséquent, le deuxième membre tout entier est divisible par u_n^2, c.-à-d. congru à 0 modulo u_n^2, ce qu'il fallait démontrer.

35. Soit p un nombre premier. Comme on l'a déjà démontré au n° 1, u_{np} est divisible par u_n. Donc, lorsqu'on passe de u_n à u_{np}, premièrement, de nouveaux diviseurs premiers peuvent apparaître, et deuxièmement, les exposants des anciens diviseurs premiers de u_n peuvent s'accroître. Nous allons démontrer un théorème, d'où il découle que, de tous les diviseurs premiers de u_n p, est le seul dont l'exposant puisse augmenter. Si $p \neq 2$, son exposant ne peut augmenter que d'une unité, si $p = 2$, son exposant peut augmenter de 2 unités au plus.

● THÉORÈME. *Si q est un diviseur premier de u_n différent de p, alors $\frac{u_{np}}{u_n}$ n'est pas divisible par q.*

Si p est un diviseur premier impair de u_n, alors $\frac{u_{np}}{u_n}$ est divisible par p et non divisible par p^2.

Si u_n est divisible par 4, alors $\frac{u_{2n}}{u_n}$ est divisible par 2 et non divisible par 4.

Si u_n est divisible par 2 et non divisible par 4, alors $\frac{u_{2n}}{u_n}$ est divisible par 4 et non divisible par 8.

● DÉMONSTRATION. Si l'on pose $m = p$ dans le lemme précédent, on obtient que

$$u_{np} - u_{n+1}^p + u_{n-1}^p \text{ est divisible par } u_n^2.$$

Mais u_{np} est divisible par u_n en vertu du nº 1 ; d'autre part,

$$u_{n+1}^p - u_{n-1}^p = (u_{n+1} - u_{n-1})(u_{n+1}^{p-1} + u_{n+1}^{p-2}u_{n-1} + \ldots + u_{n-1}^{p-1}) =$$
$$= u_n (u_{n+1}^{p-1} + u_{n+1}^{p-2}u_{n-1} + \ldots + u_{n-1}^{p-1}).$$

Par suite, la différence

$$\frac{u_{np}}{u_n} - (u_{n+1}^{p-1} + u_{n+1}^{p-2}u_{n-1} + \ldots + u_{n-1}^{p-1}) \tag{2.31}$$

est divisible par u_n^2.

Premièrement, il en résulte que la différence (2.31) est divisible par u_n. Cela signifie que

$$\frac{u_{np}}{u_n} \equiv u_{n+1}^{p-1} + u_{n+1}^{p-2}u_{n-1} + \ldots + u_{n-1}^{p-1} \pmod{u_n}. \tag{2.32}$$

D'autre part, il est évident que

$$u_{n+1} \equiv u_{n-1} \pmod{u_n}.$$

Donc, il s'ensuit de (2.32) que

$$\frac{u_{np}}{u_n} \equiv u_{n+1}^{p-1} + u_{n+1}^{p-1} + \ldots + u_{n+1}^{p-1} \pmod{u_n}.$$

Comme le second membre contient p termes, on peut écrire

$$\frac{u_{np}}{u_n} \equiv p u_{n+1}^{p-1} \pmod{u_n}.$$

Par conséquent, tout diviseur commun aux nombres $\frac{u_{np}}{u_n}$ et u_n doit diviser p, et inversement. Cela signifie que

$$\text{PGCD}\left(\frac{u_{np}}{u_n},\ u_n\right)=\text{PGCD}(p,\ u_n).$$

Soit à présent q un diviseur premier de u_n différent de p. Alors $\text{PGCD}(p,\ u_n)$ n'est pas divisible par q.

Par suite, $\text{PGCD}\left(\frac{u_{np}}{u_n},\ u_n\right)$ n'est pas non plus divisible par q. Comme q divise u_n, il ne peut pas diviser $\frac{u_{np}}{u_n}$, et la première partie du théorème est démontrée.

Deuxièmement, de la divisibilité de la différence (2.31) par u_n^2 il résulte que

$$\frac{u_{np}}{u_n}\equiv u_{n+1}^{p-1}+u_{n+1}^{p-2}u_{n-1}+\ldots+u_{n-1}^{p-1}\ (\text{mod}\ p^2).$$

Soit

$$u_{n+1}\equiv r_1p+r'\ (\text{mod}\ p^2),$$
$$u_{n-1}\equiv r_2p+r''\ (\text{mod}\ p^2),$$

où $0\leqslant r_1,\ r_2,\ r',\ r''<p$ (comme la différence $u_{n+1}-u_{n-1}$ est égale à u_n, c.-à-d. qu'elle est divisible par p, les restes r' et r'' doivent être égaux; on peut donc poser $r'=r''=r$; en outre, $r\neq 0$, car ni u_{n-1}, ni u_{n+1} ne sont divisibles par p).

Alors

$$\frac{u_{np}}{u_n}\equiv(r_1p+r)^{p-1}+(r_1p+r)^{p-2}(r_2p+r)+\ldots+$$
$$+(r_1p+r)^{p-k}(r_2p+r)^{k-1}+\ldots+(r_2p+r)^{p-1}\ (\text{mod}\ p^2).$$

Chassons les parenthèses dans le deuxième membre et rejetons les termes divisibles par p^2. Le terme

$$(r_1p+r)^{p-k}(r_2p+r)^{k-1}$$

donne alors

$$C_{p-k}^1r_1pr^{p-k-1}r^{k-1}+r^{p-k}C_{k-1}^1r_2pr^{k-2}+r^{p-k}r^{k-1}$$

ou

$$(p-k)\,pr_1r^{p-2}+(k-1)\,pr_2r^{p-2}+r^{p-1}.$$

En sommant cette expression sur tous les termes, c.-à-d. pour $k = 1, \ldots, p$, on obtient

$$\frac{u_{np}}{u_n} \equiv \frac{p(p-1)}{2} pr_1 r^{p-2} + \frac{p(p-1)}{2} pr_2 r^{p-2} + pr^{p-1} \pmod{p^2}. \quad (2.33)$$

Si $p \neq 2$, $\frac{p-1}{2}$ est un nombre entier. C'est pourquoi les deux premiers termes du second membre de (2.33) sont divisibles par p^2 et on a donc

$$\frac{u_{np}}{u_n} \equiv pr^{p-1} \pmod{p^2}.$$

Enfin, selon le théorème de Fermat (v. nº 20) $r^{p-1} - 1$ est divisible par p, de sorte que $pr^{p-1} - p$ est divisible par p^2. Si l'on en tient compte, on obtient en définitive

$$\frac{u_{np}}{u_n} \equiv p \pmod{p^2}.$$

Ainsi, $\frac{u_{np}}{u_n}$ divisé par p^2 donne p pour reste, c.-à-d. $\frac{u_{np}}{u_n}$ est divisible par p et non divisible par p^2. La deuxième partie du théorème est donc démontrée.

Soit à présent $p = 2$. La congruence (2.33) peut alors s'écrire

$$\frac{u_{2n}}{u_n} \equiv 2(r_1 + r_2 + r) \pmod 4. \quad (2.34)$$

Si u_n est divisible par 4, on voit d'après la suite de restes (2.2) que, dans ce cas, étant divisés par 4, u_{n-1} comme u_{n+1} donnent 1 pour reste. Donc, on a $r_1 = r_2 = 0$, $r = 1$, et la congruence (2.34) devient

$$\frac{u_{2n}}{u_n} \equiv 2 \pmod 4.$$

Ceci démontre la troisième partie du théorème.

Enfin, supposons que u_n ne soit pas divisible par 4. La suite (2.2) montre qu'alors $r_1 = 0$, $r_2 = 1$ et $r = 1$. Par suite, la congruence (2.34) devient

$$\frac{u_{2n}}{u_n} \equiv 0 \pmod 4.$$

Il reste à montrer que $\frac{u_{2n}}{u_n}$ n'est pas divisible par 8. Dans le cas contraire, u_{2n} serait divisible par 16. Mais alors, en vertu du nº 13,

$2n$ doit être divisible par 12, c.-à-d. que n doit être divisible par 6. Ceci à son tour implique que u_n doit être divisible par u_6, c.-à-d. par 8, ce qui est en contradiction avec l'hypothèse (selon laquelle u_n n'est pas divisible même par 4).

Le théorème est entièrement démontré.

36. Maintenant nous pouvons aborder la démonstration de l'existence des diviseurs propres des termes de la suite de Fibonacci.

● THÉORÈME. *Tout terme de la suite de Fibonacci, excepté u_1, u_2, u_6 et u_{12}, possède au moins un diviseur propre.*

● DÉMONSTRATION. Considérons le terme u_n. Soit

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

la décomposition canonique du nombre n.

Cherchons le plus petit commun multiple des termes

$$u_{\frac{n}{p_1}}, \ u_{\frac{n}{p_2}}, \ \dots, \ u_{\frac{n}{p_k}}. \tag{2.35}$$

D'après le nº 32,

PPCM=

$$= \frac{u_{\frac{n}{p_1}} u_{\frac{n}{p_2}} \dots u_{\frac{n}{p_k}} \cdot \mathrm{PGCD}\left(u_{\frac{n}{p_1}}, u_{\frac{n}{p_2}}, u_{\frac{n}{p_3}}\right) \dots}{\mathrm{PGCD}\left(u_{\frac{n}{p_1}}, u_{\frac{n}{p_2}}\right) \dots \mathrm{PGCD}\left(u_{\frac{n}{p_{k-1}}}, u_{\frac{n}{p_k}}\right) \mathrm{PGCD}\left(u_{\frac{n}{p_1}}, u_{\frac{n}{p_2}}, u_{\frac{n}{p_3}}, u_{\frac{n}{p_4}}\right) \dots} \tag{2.36}$$

Or, pour tout r et quels que soient $i_1, i_2, \dots, i_r$ distincts, on a

$$\mathrm{PGCD}\left(u_{\frac{n}{p_{i_1}}}, u_{\frac{n}{p_{i_2}}}, \dots, u_{\frac{n}{p_{i_r}}}\right) = u_{\mathrm{PGCD}\left(\frac{n}{p_{i_1}}, \frac{n}{p_{i_2}}, \dots, \frac{n}{p_{i_r}}\right)} =$$

$$= u_{\frac{n}{p_{i_1} p_{i_2} \dots p_{i_r}}}.$$

Donc,

$$\mathrm{PPCM} = \frac{u_{\frac{n}{p_1}} u_{\frac{n}{p_2}} \dots u_{\frac{n}{p_k}} u_{\frac{n}{p_1 p_2 p_3}} \dots}{u_{\frac{n}{p_1 p_2}} u_{\frac{n}{p_1 p_3}} \dots u_{\frac{n}{p_{k-1} p_k}} u_{\frac{n}{p_1 p_2 p_3 p_4}} \dots}.$$

Mais u_n est divisible par tous les nombres $u_{\frac{n}{p_1}}, u_{\frac{n}{p_2}}, \ldots, u_{\frac{n}{p_k}}$, donc par leur plus petit commun multiple

$$u_n = \text{PPCM } t.$$

Tout diviseur premier du PPCM divise l'un des nombres (2.35) et représente donc un diviseur impropre de u_n. Par conséquent, tous les diviseurs propres de u_n doivent diviser t. D'après le théorème du nº 35, de tous les diviseurs premiers impropres de u_n seuls $p_1, p_2, \ldots, p_k$ peuvent entrer dans t; de plus, chacun de ces nombres entre dans t avec un exposant inférieur ou égal à 1, excepté le nombre 2, qui peut entrer avec l'exposant 2.

En démontrant l'inégalité

$$t > \underset{\times}{2}\, p_1 p_2 \ldots p_k$$

(ici et dans la suite, la croix au-dessous du nombre 2 signifie que le nombre 2 n'est pris en considération que dans le cas où les nombres $p_1, p_2, \ldots, p_k$ comptent déjà un 2), nous prouverons que le terme u_n possède des diviseurs propres.

Ainsi démontrons que

$$t = \frac{u_n u_{\frac{n}{p_1 p_2}} u_{\frac{n}{p_1 p_3}} \ldots u_{\frac{n}{p_{k-1} p_k}} u_{\frac{n}{p_1 p_2 p_3 p_4}} \ldots}{u_{\frac{n}{p_1}} u_{\frac{n}{p_2}} \ldots u_{\frac{n}{p_k}} u_{\frac{n}{p_1 p_2 p_3}} \ldots} > \underset{\times}{2}\, p_1 p_2 \ldots p_k.$$

Au nº 21 du § 1 on a établi que

$$\frac{1}{\sqrt{5}}\alpha^{n-\frac{1}{n}} \leqslant u_n \leqslant \frac{1}{\sqrt{5}}\alpha^{n+\frac{1}{n}}.$$

Donc, si l'on remplace tous les nombres de Fibonacci figurant au numérateur par $\frac{1}{\sqrt{5}}\alpha^{n-\frac{1}{n}}$ et ceux du dénominateur par $\frac{1}{\sqrt{5}}\alpha^{n+\frac{1}{n}}$, la fraction ne peut que diminuer. En démontrant l'inégalité pour la nouvelle fraction, nous établissons plus qu'il nous fallait. En effectuant les subs-

titutions indiquées et en simplifiant par $\left(\frac{1}{\sqrt{5}}\right)^{2^k}$, nous obtenons

$$\frac{\alpha^{n-\frac{1}{n}}\alpha^{\frac{n}{p_1p_2}-\frac{p_1p_2}{n}}\cdots\alpha^{\frac{n}{p_{k-1}p_k}-\frac{p_{k-1}p_k}{n}}\alpha^{\frac{n}{p_1p_2p_3p_4}-\frac{p_1p_2p_3p_4}{n}}\cdots}{\alpha^{\frac{n}{p_1}-\frac{p_1}{n}}\alpha^{\frac{n}{p_2}-\frac{p_2}{n}}\cdots\alpha^{\frac{n}{p_k}-\frac{p_k}{n}}\alpha^{\frac{n}{p_1p_2p_3}-\frac{p_1p_2p_3}{n}}\cdots}>$$

$$> \underset{\times}{2}p_1p_2\ldots p_k,$$

ou

$$\frac{\alpha^{n\left(1-\frac{1}{p_1}-\frac{1}{p_2}-\ldots-\frac{1}{p_k}+\frac{1}{p_1p_2}+\ldots+\frac{1}{p_{k-1}p_k}-\frac{1}{p_1p_2p_3}-\ldots\right)}}{\alpha^{\frac{1}{n}(1+p_1+p_2+\ldots+p_k+p_1p_2+\ldots+p_{k-1}p_k+p_1p_2p_3+\ldots)}}>$$

$$> \underset{\times}{2}p_1p_2\ldots p_k,$$

ou encore

$$\alpha^{n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)-\frac{1}{n}(1+p_1)(1+p_2)\ldots(1+p_k)}>$$

$$> \underset{\times}{2}p_1p_2\ldots p_k,$$

ou, enfin, en passant aux logarithmes,

$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)-\frac{1}{n}(1+p_1)(1+p_2)\ldots$$

$$\ldots(1+p_k)>\log_\alpha \underset{\times}{2}p_1p_2\ldots p_k.$$

En nous rappelant la décomposition canonique de n, nous pouvons mettre l'inégalité précédente sous la forme:

$$p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)-$$

$$-\frac{p_1+1}{p_1^{\alpha_1}}\,\frac{p_2+1}{p_2^{\alpha_2}}\cdots\frac{p_k+1}{p_k^{\alpha_k}}>\log_\alpha \underset{\times}{2}p_1p_2\ldots p_k.$$

L'expression $p_1^{\alpha_1-1}(p_1-1)\ldots p_k^{\alpha_k-1}(p_k-1)$ est désignée d'habitude par $\varphi(n)$. La fonction qu'elle définit est appelée fonction d'Euler. Elle jouit de nombreuses propriétés aussi intéressantes qu'importantes.

Avec la notation de la fonction d'Euler on peut écrire

$$\varphi(n) > \frac{p_1+1}{p_1^{\alpha_1}}\,\frac{p_2+1}{p_2^{\alpha_2}}\cdots\frac{p_k+1}{p_k^{\alpha_k}} + \log_\alpha \underset{\times}{2} p_1 p_2 \ldots p_k. \qquad (2.36)$$

Il reste à vérifier pour quelles valeurs entières positives de n l'inégalité écrite est satisfaite. Nous dirons que ces valeurs sont « bonnes » pour les distinguer des « mauvaises » valeurs de n qui ne satisfont pas à l'inégalité (2.36). Il est évident que pour les bonnes valeurs de n les termes u_n possèdent des diviseurs propres. Il importe de souligner que la réciproque peut ne pas être vraie: la validité de l'inégalité (2.36) est une condition suffisante, mais pas nécessaire pour que u_n ait des diviseurs propres. Par conséquent, on doit essayer les termes de la suite de Fibonacci ayant de mauvais numéros (on en compte 10 au total) pour établir l'existence des diviseurs propres. Cette vérification révèle que parmi ces 10 nombres il y a 6 qui ont des diviseurs propres et 4 (ceux qui sont énumérés dans l'énoncé du théorème) qui n'en ont pas.

On constate « à vue d'œil » qu'avec la croissance de n le premier membre de (2.36) croît plus vite que le second. Donc, dès le début il faut admettre que l'inégalité (2.36) peut ne pas avoir lieu seulement pour des valeurs pas trop grandes de n. Malgré la tendance générale à l'accroissement, les deux membres de l'inégalité changent cependant avec l'augmentation de n de façon très irrégulière, de sorte qu'on doute fort qu'on puisse appliquer un raisonnement par récurrence direct. Aussi il nous semble naturel d'adopter le programme d'action suivant. Etablissons un procédé permettant d'énumérer (écrire) successivement tous les entiers naturels de façon que chaque bon nombre soit nécessairement suivi d'un bon nombre. Si à une étape quelconque tous les nombres obtenus sont bons, alors tous les nombres suivants le seront également. Par conséquent, tous les mauvais nombres doivent être énumérés avant cette étape. Le lecteur peut remarquer que cette façon de raisonner est une variante de la démonstration par récurrence.

Démontrons préalablement les trois propositions suivantes.

1. Soient $p_1, p_2, \ldots, p_k, \ldots$ tous les nombres premiers énumérés dans l'ordre de croissance (c.-à-d. $p_1 = 2$, $p_2 = 3$, etc.). Alors si le nombre $n = p_1p_2 \ldots p_k$ est bon et $p_{k+1} > 3$, le nombre $p_1p_2 \ldots p_kp_{k+1}$ est également bon.

En effet, dans ce cas on a

$$n = p_1p_2 \ldots p_k,$$
$$\varphi(n) = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$$

et par hypothèse on doit avoir

$$(p_1-1)(p_2-1)\ldots(p_k-1) >$$
$$> \left(1+\frac{1}{p_1}\right)\left(1+\frac{1}{p_2}\right)\cdots\left(1+\frac{1}{p_k}\right) + \log_\alpha \underset{\times}{2} p_1p_2\ldots p_k. \qquad (2.37)$$

Pour obtenir l'inégalité correspondante pour le produit $p_1p_2 \dots$ $\dots p_kp_{k+1}$, il faut multiplier le premier terme du second membre de (2.37) par le nombre $1+\frac{1}{p_{k+1}}$, qui est inférieur à 2, et ajouter $\log_a p_{k+1}$ au second terme. Or, le nombre $p_1p_2 \dots p_k - 1$ est premier avec chacun des nombres premiers $p_1p_2, \dots, p_k$. Par conséquent, chaque diviseur propre q de $p_1, p_2 \dots p_k = 1$ est supérieur à chacun des nombres $p_1, p_2, \dots, p_k$ et donc supérieur ou égal à p_{k+1}. Donc,

$$p_{k+1} < p_1p_2 \dots p_k$$

et à plus forte raison

$$p_{k+1} < 2p_1p_2 \dots p_k,$$

d'où

$$\log_a p_{k+1} < \log_a 2p_1p_2 \dots p_k.$$

Par suite, si on ajoute $\log_a p_{k+1}$ au deuxième terme, celui-ci augmente moins de deux fois.

Ainsi, le second membre ne peut pas augmenter plus de 2 fois. Quant au premier membre, il est multiplié par le nombre $p_{k+1} - 1$ qui est plus grand que 2. Donc, de (2.37) il résulte que

$$(p_1-1)\dots(p_k-1)(p_{k+1}-1) >$$
$$> \left(1+\frac{1}{p_1}\right)\dots\left(1+\frac{1}{p_k}\right)\left(1+\frac{1}{p_{k+1}}\right)+\log_a 2p_1 \dots p_kp_{k+1},$$

ce qu'il fallait démontrer.

2. Si $n = p_1p_2 \dots p_k$, où $p_1, p_2, \dots, p_k$ sont des nombres premiers distincts arbitraires, n un bon nombre et q un nombre premier quelconque différent de $p_1, p_2, \dots, p_k$ et supérieur à p_1, alors $qp_2 \dots p_k$ est également un bon nombre.

En effet, dans ce cas l'inégalité (2.36) prend de nouveau la forme (2.37). Remplacer ici p_1 par q équivaut à multiplier le premier membre de (2.37) par $\frac{q-1}{p_1-1}$ et, dans son deuxième membre, multiplier le premier terme par $\frac{1+\frac{1}{q}}{1+\frac{1}{p_1}}$ et ajouter $\log_a \frac{q}{p_1}$ au second. Comme $q > p_1$, une telle multiplication ne peut que faire diminuer le premier terme.

Ensuite, puisque $\frac{q}{p_1} > 1$, on a

$$\frac{q-1}{p_1-1} > \frac{q}{p_1}$$

et donc

$$\frac{q-1}{p_1-1} > \log_\alpha \frac{q}{p_1}.$$

Le second membre de (2.37) est plus grand que 1 (ne serait-ce parce que tous les nombres premiers, à partir de 2, sont plus grands que α^2). Le premier membre étant plus grand que le second est lui aussi supérieur à 1. Mais si on multiplie le premier membre (qui est plus grand que 1) par un nombre plus grand que 1 et si on ajoute au second membre un nombre plus petit, l'inégalité (2.37) ne peut que se renforcer.

3. Si $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ est un bon nombre, alors $p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots$ $\ldots p_k^{\alpha_k}$ l'est également.

Pour le démontrer il suffit de remarquer que si on remplace dans l'inégalité

$$p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1) >$$
$$> \frac{p_1+1}{p_1^{\alpha_1}}\,\frac{p_2+1}{p_2^{\alpha_2}}\ldots\frac{p_k+1}{p_k^{\alpha_k}} + \log_\alpha \frac{2p_1p_2\ldots p_k}{x}$$

l'exposant α_1 par le nombre plus grand α_1+1, le premier membre augmente et le second diminue. Donc, par une telle transformation un bon nombre ne peut avoir pour image qu'un bon nombre.

Ainsi, nous avons à notre disposition trois opérations sur les nombres, soit trois procédés de passage d'un nombre à un autre. Ceci étant, on ne peut passer d'un bon nombre qu'à un autre bon nombre.

La première de ces opérations consiste à construire la suite 1, 2, 6, 30, 210, . . . ; la deuxième à remplacer, dans les nombres dont la décomposition canonique ne contient que les premières puissances des facteurs premiers, tout diviseur premier par un autre plus grand (par souci de clarté, on convient de le remplacer par le nombre premier « supérieur » le plus proche) qui ne fait pas partie de la décomposition ; la troisième opération fait croître d'une unité un exposant quelconque dans la décomposition canonique. En partant du nombre 1, on peut énumérer à l'aide de ces opérations tous les entiers naturels. Certains nombres figurent dans cette liste plus d'une fois, mais cette circonstance ne joue aucun rôle. Il importe que chaque nombre soit pris en considération au moins une fois.

Commençons donc à énumérer les entiers naturels de la façon indiquée ci-dessus. Utilisons d'abord la première opération.

Le nombre 1 est mauvais, car pour $n = 1$ l'inégalité (2.36) prend la forme contradictoire suivante:

$$1 > 1 + \log_\alpha \underset{\times}{2} = 1 + \log_\alpha 1 = 1$$

(nous considérons toujours que tout produit de zéro facteurs est égal à 1).

La première opération, appliquée au nombre 1, donne 2. Pour $n = 2$ l'inégalité (2.36) prend la forme

$$1 > \frac{3}{2} + \log_\alpha \underset{\times}{2} = \frac{3}{2} + \log_\alpha 4\,;$$

comme elle est fausse, le nombre 2 est aussi mauvais.

Les nombres suivants, 6 et 30, sont eux aussi mauvais, car pour eux on a respectivement

$$\varphi(6) = 2 < \frac{3}{2}\cdot\frac{4}{3} + \log_\alpha 12 = 2 + \log_\alpha 12,$$

$$\varphi(30) = 8 < \frac{3}{2}\cdot\frac{4}{3}\cdot\frac{6}{5} + \log_\alpha 60 \approx 2{,}4 + 8{,}5.$$

Par contre, le nombre $2\cdot3\cdot5\cdot7 = 210$ est bon, puisque

$$\varphi(210) = 48 > \frac{3}{2}\cdot\frac{4}{3}\cdot\frac{6}{5}\cdot\frac{8}{7} + \log_\alpha 420 \approx 2{,}7 + 12{,}5.$$

Donc, tous les nombres suivants, obtenus par la première opération, sont bons. Appliquons maintenant la deuxième et la troisième opération.

Appliquées au nombre 2, elles donnent les nombres 3 et 4 qui sont mauvais, car

$$\varphi(3) = 2 < \frac{4}{3} + \log_\alpha 3 \approx 1{,}3 + 2{,}3,$$

$$\varphi(4) = 2 < \frac{3}{2} + \log_\alpha 4 \approx 1{,}5 + 2{,}9.$$

L'application de ces opérations au nombre 3 donne respectivement 5 et 9. On vérifie facilement que 5 est mauvais et 9 est bon, de sorte que les transformations suivantes de 9 ne nous intéressent pas. Quant à 5, il se transforme par la deuxième opération en 7 et par la troisième en 25. Ces nombres étant bons tous les deux, il en est de même de tous leurs suivants, ce qui nous dispense de les étudier.

La troisième opération, appliquée au nombre 4, conduit au nombre 8 qui est bon.

Ainsi l'application successive de la deuxième et de la troisième opération au nombre 2 donne d'abord les mauvais nombres 3, 4 et 5, puis de bons nombres.

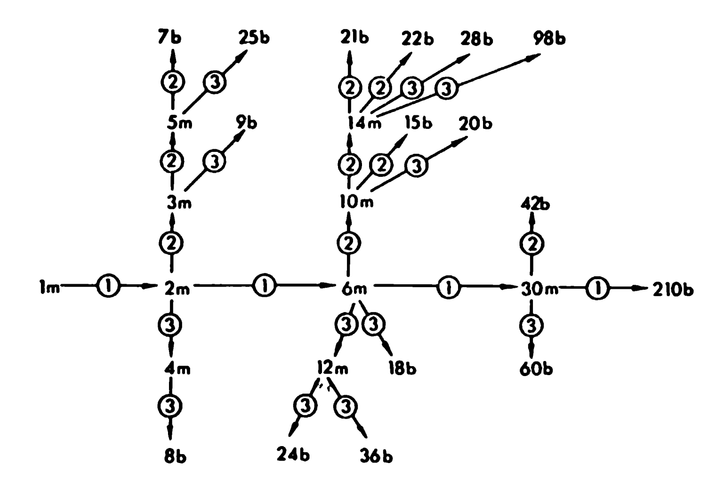


Fig. 1

Examinons maintenant le nombre 6. En lui appliquant la deuxième opération, on obtient le mauvais nombre 10, suivi de deux bons nombres (20 et 15) et d'un mauvais (14). Ce dernier est suivi de bons nombres 21 et 22 (obtenus par la deuxième opération) et de bons nombres 28 et 98 (obtenus par la troisième opération).

La troisième opération, appliquée à 6, donne le bon nombre 18 et le mauvais 12. Par la troisième opération on obtient de 12 les bons nombres 24 et 36 ; la deuxième opération ne s'applique pas à 12, car celui-ci est divisible par le carré du nombre premier 2.

Enfin, tous les nombres que l'on obtient de 30 (respectivement 210, 42 et 60) sont bons. Les raisonnements précédents sont illustrés par le schéma ci-dessus suivant (fig. 1).

Finalement, on aboutit à la liste suivante de mauvais nombres:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 14,\ 30.$$

Les termes correspondants de la suite de Fibonacci sont

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 55,\ 144,\ 377,\ u_{30}.$$

Il est évident que u_3, u_4, u_5, u_{10} et u_{14} ont pour diviseurs propres respectivement 2, 3, 5, 11 et 29. En écrivant tous les termes de la suite de Fibonacci jusqu'à u_{30} et leurs décompositions en facteurs

premiers, on pourrait vérifier directement que u_{30} possède un diviseur propre. Mais on n'en a pas besoin. En effet, d'après le théorème du n° 22 u_{30} est divisible par 31 (car 31 est un nombre premier de la forme $5t + 1$). D'autre part, ni $u_6 = 8$, ni $u_{10} = 55$, ni $u_{15} = 610$ ne sont pas divisibles par 31. Donc, 31 est un diviseur propre de u_{30}.

Il reste les nombres $u_1 = 1$, $u_2 = 1$, $u_6 = 8$ et $u_{12} = 144$ qui, évidemment, n'ont pas de diviseurs propres.

Le théorème est démontré.

37. Contrairement aux quatre termes de la suite de Fibonacci qui n'ont pas de diviseurs propres, il existe d'autres termes qui en possèdent plusieurs. Par exemple, pour u_{19} de tels diviseurs sont les nombres 37 et 113, pour u_{27} les nombres 53 et 109, etc. Est-ce qu'il y a beaucoup de termes de la suite de Fibonacci qui possèdent deux ou plusieurs diviseurs propres? On n'en sait absolument rien.

Il est naturel de se demander quel est le numéro n du terme dont le diviseur propre est le nombre premier donné p.

Du n° 25 il résulte que $n \leqslant p - 1$, si p est de la forme $5t \pm 1$, et $n \leqslant p + 1$, si p est de la forme $5t \pm 2$. Cependant, on ne connaît pour le moment aucune formule permettant de calculer directement les numéros des termes ayant pour diviseur propre le nombre p donné à l'avance.

Nous avons démontré au n° 9 que sauf u_4 tous les termes de la suite de Fibonacci dont les numéros sont des nombres composés sont eux-mêmes des nombres composés. La réciproque est inexacte, car, par exemple, $u_{19} = 4181 = 37 \cdot 113$. Une question se pose à savoir si l'ensemble de tous les nombres premiers de Fibonacci est fini ou infini, c.-à-d. si parmi ces nombres il existe un plus grand. Ce problème est loin d'être résolu.

§ 3 SUITE DE FIBONACCI ET FRACTIONS CONTINUES

1. Considérons l'expression

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + \cfrac{1}{q_n}}}}} \qquad (3.1)$$

où $q_1, q_2, \ldots, q_n$ sont des entiers *positifs* et q_0 un entier *naturel*, c'est-à-dire que q_0 peut être égal à zéro, ce qui est impossible pour les nombres $q_1, q_2, \ldots, q_n$. Dans la suite nous sous-entendrons toujours cette propriété de q_0.

L'expression (3.1) est la *fraction continue* et les nombres $q_0, q_1, q_2, \ldots, q_n$ les *quotients incomplets* de cette fraction.

Les fractions continues trouvent de nombreuses applications dans les questions les plus diverses des mathématiques.

La représentation d'un nombre quelconque par une fraction continue est la *décomposition* de ce nombre en fraction continue.

Comment trouver les quotients incomplets d'une fraction continue obtenue par la décomposition de la fraction ordinaire $\frac{a}{b}$?

Considérons l'algorithme d'Euclide appliqué aux nombres a et b:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\ldots\ldots\ldots\ldots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n. \end{aligned} \tag{3.2}$$

La première égalité donne:

$$\frac{a}{b} = q_0 + \frac{r_1}{b} = q_0 + \frac{1}{\frac{b}{r_1}}.$$

De la deuxième égalité on déduit

$$\frac{b}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}},$$

d'où

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{r_1}{r_2}}}.$$

La troisième égalité nous fournit

$$\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \cfrac{1}{\cfrac{r_2}{r_3}},$$

donc

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{r_2}{r_3}}}}.$$

Et ainsi de suite jusqu'à ce qu'on aboutisse au résultat

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{}{\ddots + \cfrac{1}{q_n}}}}.$$

D'après l'idée de l'algorithme d'Euclide, q_n est supérieur à 1. (En effet, si q_n était égal à 1, on aurait $r_{n-1} = r_n$ et r_{n-2} serait divisible par r_{n-1}, c'est-à-dire que l'algorithme serait arrêté à l'avant-dernier pas.)

On peut donc considérer au lieu de q_n l'expression $(q_n - 1) + \frac{1}{1}$, c'est-à-dire prendre la différence $(q_n - 1)$ pour l'avant-dernier quotient incomplet et l'unité pour le dernier. Cette convention s'avérera très utile dans la suite.

2. Il est clair que toute fraction rationnelle $\frac{a}{b}$ peut être décomposée en fraction continue. Montrons que cette décomposition est unique, c'est-à-dire que si deux fractions continues sont égales, leurs quotients incomplets correspondants le sont aussi.

Soient ω et ω' deux fractions continues telles que $\omega = \omega'$ et soient $q_0, q_1, \ldots, q_n$ et $q'_0, q'_1, \ldots, q'_n$ respectivement leurs quotients incomplets. Alors $q_0 = q'_0$, $q_1 = q'_1$, etc. En effet, q_0 est la partie entière de ω et q'_0 celle de ω', donc $q_0 = q'_0$. Les fractions continues ω et ω' s'écrivent respectivement

$$q_0 + \frac{1}{\omega_1} \quad \text{et} \quad q'_0 + \frac{1}{\omega'_1},$$

où ω_1 et ω'_1 sont encore les fractions continues. Les égalités $\omega = \omega'$ et $q_0 = q'_0$ entraînent $\omega_1 = \omega'_1$. Les parties entières de ω_1 et de ω'_1 sont donc elles aussi égales ($q_1 = q'_1$). Et ainsi de suite ($q_2 = q'_2$, $q_3 = q'_3$, etc.).

3. Soit

$$\omega = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_n}}} \tag{3.3}$$

une fraction continue. Considérons les nombres

$$q_0, \quad q_0 + \frac{1}{q_1}, \quad q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}, \quad \ldots$$

Il est toujours possible de les mettre sous la forme des fractions irréductibles

$$\frac{P_0}{Q_0}=\frac{q_0}{1},$$

$$\frac{P_1}{Q_1}=q_0+\frac{1}{q_1},$$

$$\frac{P_2}{Q_2}=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2}},$$

. . . .

$$\frac{P_n}{Q_n}=\omega.$$

Ils s'appellent alors les *fractions correspondant* à la fraction continue ω. Constatons que $\frac{P_{k+1}}{Q_{k+1}}$ est l'expression modifiée de $\frac{P_k}{Q_k}$, où le dernier quotient incomplet q_k est remplacé par la somme $q_k+\frac{1}{q_{k+1}}$.

4. Le lemme ci-dessous est fort important pour la théorie des fractions continues.

● LEMME. *Quelle que soit la fraction continue* (3.3), *les trois relations suivantes sont toujours vérifiées*:

$$P_{k+1}=P_kq_{k+1}+P_{k-1}, \tag{3.4}$$

$$Q_{k+1}=Q_kq_{k+1}+Q_{k-1}, \tag{3.5}$$

$$P_{k+1}Q_k-P_kQ_{k+1}=(-1)^k. \tag{3.6}$$

Raisonnons par récurrence et examinons d'abord le cas $k=1$:

$$\frac{P_1}{Q_1}=q_0+\frac{1}{q_1}=\frac{q_0q_1+1}{q_1}.$$

Puisque les nombres $q_0q_1 + 1$ et q_1 sont premiers entre eux, la fraction $\frac{q_0q_1+1}{q_1}$ est irréductible. Par définition, la fraction $\frac{P_1}{Q_1}$ est elle aussi irréductible. Or, on sait que deux fractions irréductibles étant égales, leurs numérateurs et leurs dénominateurs sont respectivement égaux. Par conséquent, $P_1 = q_0q_1 + 1$ et $Q_1 = q_1$. Considérons la fraction

$$\frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}} = \frac{q_0(q_1q_2+1)+q_2}{q_1q_2+1}. \qquad (3.7)$$

Selon le numéro 10 du § 2 le plus grand commun diviseur des nombres $q_0(q_1q_2 + 1) + q_2$ et $q_1q_2 + 1$ est égal au PGCD $(q_2, q_1q_2 + 1)$ ou encore au PGCD $(q_2, 1)$, c'est-à-dire à 1. Donc le deuxième membre de l'égalité (3.7) est une fraction irréductible et on a

$$P_2 = q_0(q_1q_2 + 1) + q_2 = (q_0q_1 + 1)q_2 + q_0 = P_1q_2 + P_0$$

et

$$Q_2 = q_1q_2 + 1 = Q_1q_2 + Q_0.$$

On vérifie aisément l'égalité

$$P_2Q_1 - P_1Q_2 = (-1)^1.$$

$k = 1$ satisfait donc aux égalités (3.4), (3.5), (3.6).

Supposons maintenant que les égalités (3.4), (3.5), (3.6) soient justes et considérons la fraction correspondante

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{P_kq_{k+1} + P_{k-1}}{Q_kq_{k+1} + Q_{k-1}}.$$

$\frac{P_{k+2}}{Q_{k+2}}$ s'exprime, on l'a dit, à l'aide de la fraction $\frac{P_{k+1}}{Q_{k+1}}$, où q_{k+1} est remplacé par $q_{k+1} + \frac{1}{q_{k+2}}$. Puisque la quantité q_{k+1} ne figure pas dans les expressions de P_k, Q_k, P_{k-1} et Q_{k-1}, nous avons

$$\frac{P_{k+2}}{Q_{k+2}} = \frac{P_k\left(q_{k+1}+\frac{1}{q_{k+2}}\right)+P_{k-1}}{Q_k\left(q_{k+1}+\frac{1}{q_{k+2}}\right)+Q_{k-1}},$$

ou, d'après les suppositions (3.4) et (3.5),

$$\frac{P_{k+2}}{Q_{k+2}} = \frac{P_{k+1}q_{k+2}+P_k}{Q_{k+1}q_{k+2}+Q_k}. \tag{3.8}$$

Démontrons que le second membre de (3.8) est une fraction irréductible. Il suffit de montrer que son numérateur et son dénominateur sont des nombres premiers entre eux.

Supposons que les nombres $P_{k+1}q_{k+2} + P_k$ et $Q_{k+1}q_{k+2} + Q_k$ aient un diviseur commun $d > 1$. On en déduit que l'expression

$$(P_{k+1}q_{k+2} + P_k)\, Q_{k+1} - (Q_{k+1}q_{k+2} + Q_k)\, P_{k+1}$$

doit elle aussi être divisible par d, ce qui contredit la supposition (3.6).

Ainsi, le second membre de (3.8) est une fraction irréductible, et la relation (3.8) est donc une égalité de deux fractions irréductibles. On peut écrire

$$P_{k+2} = P_{k+1}q_{k+2} + P_k,$$
$$Q_{k+2} = Q_{k+1}q_{k+2} + Q_k.$$

Il ne nous reste qu'à démontrer l'égalité

$$P_{k+2}Q_{k+1} - P_{k+1}Q_{k+2} = (-1)^{k+1}. \tag{3.9}$$

Tout ce qui précède nous autorise à écrire:

$$P_{k+2}Q_{k+1} - P_{k+1}Q_{k+2} = P_{k+1}q_{k+2}Q_{k+1} + P_kQ_{k+1} - - P_{k+1}q_{k+2}Q_{k+1} - P_{k+1}Q_k,$$

et la relation (3.9) découle immédiatement de (3.6). Le lemme est démontré.

● CONSÉQUENCE.

$$\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_kQ_{k+1}}. \tag{3.10}$$

La d é m o n s t r a t i o n est évidente.

Puisque les quotients incomplets des fractions continues sont des entiers positifs, nous pouvons appliquer le lemme et écrire:

$$P_0 < P_1 < P_2 < \ldots, \qquad Q_0 < Q_1 < Q_2 < \ldots \tag{3.11}$$

Nous préciserons plus loin cette remarque importante.

5. Servons-nous du lemme du n° 4 pour étudier toutes les fractions continues aux quotients incomplets égaux à 1. On a le théorème intéressant suivant.

● THÉORÈME. *Si une fraction continue possède n quotients incomplets dont chacun est égal à* 1, *cette fraction est égale à* $\frac{u_{n+1}}{u_n}$.

● DÉMONSTRATION. Désignons par α_n une fraction continue à n quotients incomplets égaux à l'unité. Il est évident que $\alpha_1, \alpha_2, \ldots, \alpha_n$ forment une suite de fractions correspondant à α_n.

Soit

$$\alpha_k = \frac{P_k}{Q_k}.$$

Vu que

$$\alpha_1 = 1 = \frac{1}{1}$$

et

$$\alpha_2 = 1 + \frac{1}{1} = \frac{2}{1},$$

on a $P_1 = 1$ et $P_2 = 2$. Ensuite, $P_{n+1} = P_n q_{n+1} + P_{n-1} = P_n + P_{n-1}$. Aussi $P_n = u_{n+1}$ (cf. n° 6, § 1).

De même, $Q_1 = 1$, $Q_2 = 1$ et $Q_{n+1} = Q_n q_{n+1} + Q_{n-1} = Q_n + Q_{n-1}$, de sorte que $Q_n = u_n$. Donc,

$$\alpha_n = \frac{u_{n+1}}{u_n}. \tag{3.12}$$

Nous laissons au lecteur le soin de comparer ce résultat aux formules (1.10) et (3.6).

6. Soient deux fractions continues

$$\omega = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots}} \quad \text{et} \quad \omega' = q'_0 + \cfrac{1}{q'_1 + \cfrac{1}{q'_2 + \ldots}}$$

telles que

$$q'_0 \geqslant q_0, \; q'_1 \geqslant q_1, \; q'_2 \geqslant q_2, \ldots \tag{3.13}$$

Désignons respectivement par $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots$ et par $\frac{P'_0}{Q'_0}, \frac{P'_1}{Q'_1}, \frac{P'_2}{Q'_2}, \ldots$ les fractions correspondantes.

Les inégalités (3.13) et le lemme du n° 4 (§ 3) conduisent aux relations suivantes:

$$P'_0 \geqslant P_0, \quad P'_1 \geqslant P_1, \quad P'_2 \geqslant P_2, \ldots$$

et

$$Q'_0 \geqslant Q_0, \quad Q'_1 \geqslant Q_1, \quad Q'_2 \geqslant Q_2, \ldots$$

Il est évident que la plus petite valeur de tout quotient incomplet est 1. Etant donnée une fraction continue dont tous les quotients incomplets sont égaux à 1, les numérateurs et les dénominateurs des fractions correspondantes croissent plus lentement que ceux des fractions correspondant à toute autre fraction continue.

Etudions cet accroissement. Il est évident que, mises à part les fractions continues aux quotients incomplets égaux à l'unité, ce sont les numérateurs et les dénominateurs des fractions correspondant à une fraction continue dont un quotient incomplet est 2 et tous les autres l'unité qui accusent l'accroissement le plus lent. Selon le lemme suivant, ces fractions continues sont également liées aux termes de la suite de Fibonacci.

● LEMME. *Si les quotients incomplets $q_0, q_1, \ldots, q_n$ d'une fraction continue ω sont tels que $q_0 = q_1 = q_2 = \ldots = q_{i-1} = q_{i+1} = \ldots \ldots = q_n = 1$ et $q_i = 2$ $(i \neq 0)$, on a*

$$\omega = \frac{u_{i+1}u_{n-i+3} + u_i u_{n-i+1}}{u_i u_{n-i+3} + u_{i-1}u_{n-i+1}}.$$

La d é m o n s t r a t i o n se fait par récurrence. Pour $i = 1$, on a quel que soit n:

$$\omega = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots + \cfrac{1}{1}}} \quad (n-1 \text{ quotients incomplets}).$$

D'après ce qu'on a démontré au début de ce numéro:

$$\omega = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha_{n-1}}} = 1 + \cfrac{1}{2 + \cfrac{u_{n-1}}{u_n}} =$$

$$= 1 + \cfrac{1}{\cfrac{2u_n + u_{n-1}}{u_n}} = 1 + \frac{u_n}{u_{n+2}} = \frac{u_{n+2} + u_n}{u_{n+2}}$$

ou, en posant $u_0 = 0$,

$$\omega = \frac{u_2 u_{n+2} + u_1 u_n}{u_1 u_{n+2} + u_0 u_n}.$$

La première partie du lemme est donc démontrée.

Supposons maintenant que, quel que soit n, on ait

$$\left. \begin{matrix} 1 + \cfrac{1}{1 + \ddots} \\ \qquad\qquad + 1 + \cfrac{1}{2 + \cfrac{1}{\alpha_{n-i}}} \end{matrix} \right\} i \text{ quotients incomplets} =$$

$$= \frac{u_{i+1} u_{n-i+3} + u_i u_{n-i+1}}{u_i u_{n-i+3} + u_{i-1} u_{n-i+1}}. \qquad (3.14)$$

Considérons la fraction continue

$$\left.\begin{array}{r}i+1 \text{ quotients}\\ \text{incomplets}\end{array}\right\{ \quad 1+\cfrac{1}{1+\cfrac{}{\ddots+1+\cfrac{1}{2+\cfrac{1}{\alpha_{n-i-1}}}}}.$$

Elle peut s'écrire:

$$1+\cfrac{1}{\cdots}$$

$$\left.\begin{array}{r}i \text{ quotients}\\ \text{incomplets}\end{array}\right\{ \quad 1+\cfrac{}{\ddots+1+\cfrac{1}{2+\cfrac{1}{\alpha_{n-i-1}}}}. \qquad (3.15)$$

D'après la relation (3.14), la fraction continue au-dessous de la ligne pointillée est égale à l'expression suivante:

$$\frac{u_{i+1}u_{n-i+2}+u_iu_{n-i}}{u_iu_{n-i+2}+u_{i-1}u_{n-i}}.$$

Donc toute la fraction (3.15) s'écrit:

$$1+\cfrac{1}{\cfrac{u_{i+1}u_{n-i+2}+u_iu_{n-i}}{u_iu_{n-i+2}+u_{i-1}u_{n-i}}}=$$

$$=\frac{(u_i+u_{i+1})\,u_{n-i+2}+(u_{i-1}+u_i)\,u_{n-i}}{u_{i+1}u_{n-i+2}+u_iu_{n-i}}=$$

$$=\frac{u_{i+2}u_{n-i+2}+u_{i+1}u_{n-i}}{u_{i+1}u_{n-i+2}+u_iu_{n-i}}.$$

Le lemme est démontré.

● CONSÉQUENCE. S'il y a, parmi les quotients incomplets d'une fraction continue ω, au moins n quotients différents de l'unité et si $q_0 \neq 0$, nous avons, en écrivant ω sous la forme $\frac{P}{Q}$:

$$P \geqslant u_{i+1}u_{n-i+3}+u_iu_{n-i+1} > u_{i+1}\,u_{n-i+2}+u_iu_{n-i+1}=u_{n+2}.$$

De même

$$Q > u_{n+1}.$$

Nous insistons sur le rôle du lemme du n° 4 selon lequel, lorsqu'on remplace une fraction continue par la fraction arithmétique, on obtient toujours des fractions irréductibles, et les numérateurs et les dénominateurs des fractions ne diminuent donc pas.

7. Le numéro précédent nous permet de démontrer le théorème attribuant un sens particulier à la suite de Fibonacci face à l'algorithme d'Euclide.

● THÉORÈME. *Etant donnés deux nombres a et b, le nombre d'opérations dans l'algorithme d'Euclide est égal à* $(n-1)$ *pour un certain a si* $b = u_n$ *et est inférieur à* $(n-1)$ *pour tout a si* $b < u_n$.

● DÉMONSTRATION. On vérifie aisément la première partie du théorème. Considérons $a = u_{n+1}$, c'est-à-dire le terme de la suite de Fibonacci qui suit b. Alors

$$\frac{u_{n+1}}{u_n} = \alpha_n.$$

La fraction continue α_n possède n quotients incomplets, c'est-à-dire qu'il y a $(n-1)$ opérations dans l'algorithme d'Euclide appliqué aux nombres a et b.

Démontrerons la deuxième partie du théorème par l'absurde. Supposons que le nombre d'opérations n'est pas inférieur à $(n-1)$. Mettons $\frac{a}{b}$ sous la forme d'une fraction continue ω. Il est évident que ω contiendra au moins n quotients incomplets (ce qui dépasse d'une unité le nombre d'opérations dans l'algorithme d'Euclide). Puisque b n'est pas un terme de la suite de Fibonacci, tout quotient incomplet n'est pas égal à 1. D'après la conséquence du lemme du n° 6, on a $b > u_n$, ce qui est en contradiction avec l'hypothèse.

Le théorème ci-dessus signifie que dans un certain sens l'algorithme d'Euclide appliqué aux termes voisins de la suite de Fibonacci est « le plus long ».

8. Appelons l'expression

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \dots + \cfrac{1}{q_n + \dots}}} \qquad (3.16)$$

fraction continue infinie. Les définitions et les résultats des numéros précédents s'étendent naturellement aux fractions continues infinies. Soit

$$\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}, \ldots \tag{3.17}$$

une suite (infinie) de fractions correspondantes. Nous allons démontrer que cette suite a une limite.

Etudions deux suites

$$\frac{P_0}{Q_0}, \frac{P_2}{Q_2}, \ldots, \frac{P_{2n}}{Q_{2n}}, \ldots \tag{3.18}$$

et

$$\frac{P_1}{Q_1}, \frac{P_3}{Q_3}, \ldots, \frac{P_{2n+1}}{Q_{2n+1}}, \ldots \tag{3.19}$$

D'après les relations (3.10) et (3.11),

$$\frac{P_{2n+2}}{Q_{2n+2}}-\frac{P_{2n}}{Q_{2n}}=\frac{P_{2n+2}}{Q_{2n+2}}-\frac{P_{2n+1}}{Q_{2n+1}}+\frac{P_{2n+1}}{Q_{2n+1}}-\frac{P_{2n}}{Q_{2n}}=$$
$$=\frac{-1}{Q_{2n+2}Q_{2n+1}}+\frac{1}{Q_{2n+1}Q_{2n}}>0.$$

Il s'ensuit que la suite (3.18) est croissante. De même,

$$\frac{P_{2n+3}}{Q_{2n+3}}-\frac{P_{2n+1}}{Q_{2n+1}}=\frac{1}{Q_{2n+3}Q_{2n+2}}-\frac{1}{Q_{2n+2}Q_{2n+1}}<0$$

implique que la suite (3.19) est décroissante.

Tout terme de la suite (3.19) est supérieur à tout terme de la suite (3.18). En effet, considérons les nombres

$$\frac{P_{2n}}{Q_{2n}} \text{ et } \frac{P_{2m+1}}{Q_{2m+1}},$$

et soit k un nombre impair supérieur à $2n$ et à $2m+1$. D'après (3.10), nous pouvons écrire:

$$\frac{P_k}{Q_k}>\frac{P_{k+1}}{Q_{k+1}}. \tag{3.20}$$

Puisque la suite (3.18) est croissante et celle (3.19) décroissante, l'on a :

$$\frac{P_{n+1}}{Q_{n+1}} > \frac{P_{2n}}{Q_{2n}} \tag{3.21}$$

et

$$\frac{P_k}{Q_k} < \frac{P_{2m+1}}{Q_{2m+1}}. \tag{3.22}$$

Il découle des relations (3.20), (3.21), (3.22) que

$$\frac{P_{2m}}{Q_{2m}} < \frac{P_{2m+1}}{Q_{2m+1}}.$$

Vu (3.10) et (3.11), nous pouvons en conclure

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_{n+1}Q_n} < \frac{1}{n^2};$$

aussi la différence de la $(n+1)^{\text{ième}}$ et de la $n^{\text{ième}}$ fraction correspondante tend en valeur absolue vers zéro pour n croissant.

Il résulte de tout ce qui précède que les suites (3.18) et (3.19) ont la même limite qui est aussi celle de la suite (3.17). Cette limite s'appelle la *valeur de la fraction continue infinie* (3.16).

Nous avons démontré (nº 2) l'unicité de la décomposition d'un nombre rationnel en une fraction continue. Le fait d'avoir affaire aux fractions finies n'étant pas utilisé dans nos raisonnements, nous avons établi par là même que tout nombre réel (rationnel ou irrationnel) peut être la valeur d'une fraction continue au plus.

Puisqu'un nombre rationnel se décompose en une fraction continue finie, il en découle qu'il ne peut pas être représenté sous la forme d'une fraction continue infinie. Ainsi, la valeur d'une fraction continue infinie est nécessairement un nombre irrationnel.

L'étude de la représentation des nombres irrationnels par les fractions continues est une branche très intéressante de la théorie des nombres. Nous nous bornons ici à un seul exemple lié à la suite de Fibonacci.

9. Trouvons la valeur de la fraction continue infinie

$$1+\cfrac{1}{1+\cfrac{1}{1+\dots}} \tag{3.23}$$

D'après ce qu'on vient de démontrer, cette valeur est égale à $\lim\limits_{n\to\infty} \alpha_n$, où $\alpha_n = \frac{u_{n+1}}{u_n}$. Calculons cette limite.

u_n est le nombre entier le plus proche de $\frac{\alpha^n}{\sqrt{5}}$ (n° 20, § 1). Donc,

$$u_n = \frac{\alpha^n}{\sqrt{5}} + \theta_n,$$

où $|\theta| < \frac{1}{2}$ quel que soit n.

Utilisons le résultat obtenu au numéro 5. Nous avons

$$\lim_{n\to\infty} \alpha_n = \lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \lim_{n\to\infty} \frac{\frac{\alpha^{n+1}}{\sqrt{5}} + \theta_{n+1}}{\frac{\alpha^n}{\sqrt{5}} + \theta_n} =$$

$$= \lim_{n\to\infty} \frac{\alpha + \frac{\theta_{n+1}\sqrt{5}}{\alpha^n}}{1 + \frac{\theta_n \sqrt{5}}{\alpha^n}} = \frac{\lim\limits_{n\to\infty}\left(\alpha + \frac{\theta_{n+1}\sqrt{5}}{\alpha^n}\right)}{\lim\limits_{n\to\infty}\left(1 + \frac{\theta_n\sqrt{5}}{\alpha^n}\right)}.$$

Mais $\theta_{n+1}\sqrt{5}$ est bornée (elle est inférieure à 2 en valeur absolue), et α^n croît indéfiniment pour n tendant vers l'infini puisque $\alpha > 1$. Donc,

$$\lim_{n\to\infty} \frac{\theta_{n+1}\sqrt{5}}{\alpha^n} = 0.$$

De même nous obtenons

$$\lim_{n\to\infty} \frac{\theta_n \sqrt{5}}{\alpha^n} = 0$$

et définitivement

$$\lim_{n\to\infty} \alpha_n = \alpha.$$

Lors du calcul de la valeur de la fraction continue (3.23) on peut se passer de la formule de Binet et du passage à la limite. (Dans un certain sens, le raisonnement par récurrence du nº 2, qui s'applique non seulement aux fractions continues finies, mais encore aux fractions infinies, s'avère suffisant.)

Mettons la fraction (3.23) sous la forme:

$$1+\frac{1}{x}.$$

L'expression de x elle-même est évidemment une fraction continue (3.23) telle que

$$x = 1+\frac{1}{x},$$

d'où

$$x^2 - x - 1 = 0 \tag{3.24}$$

et

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

Puisque la valeur de la fraction (3.23) ne peut pas être un nombre négatif, elle est égale à la racine positive de l'équation (3.24), c'est-à-dire $\frac{1+\sqrt{5}}{2}$, soit α.

Il résulte de l'étude précédente que le rapport de deux termes voisins de la suite de Fibonacci tend vers α avec n croissant. Ce fait peut être utilisé dans le calcul approché de la valeur de α (cf. le calcul de u_n (nº 20, § 1) et la formule (1.35)). L'erreur commise est petite même si les termes de la suite ne sont pas tellement grands. Par exemple, le calcul à 0,0001 près donne

$$\frac{u_{10}}{u_9} = \frac{55}{34} = 1,6176,$$

et $\alpha = 1,6180$. L'erreur est donc inférieure à 0,1 %.

Il faut dire que α représente le plus mauvais cas en ce qui concerne les erreurs lors du calcul approché des nombres

irrationnels à l'aide des fractions correspondantes et de leur décomposition en fractions continues. Tout autre nombre est décrit par ses fractions correspondantes d'une façon plus précise, dans un certain sens, que α. Malgré tout l'intérêt qu'elle présente, cette circonstance ne nous occupera plus.

§ 4 SUITE DE FIBONACCI ET GÉOMÉTRIE

1. Partageons le segment AB de longueur unité en deux de façon que la plus grande des deux parties soit la moyenne proportionnelle de la plus petite et de tout le segment (fig. 2).

Désignons par x la longueur de C_1B. La longueur de AC_1 est évidemment égale à $1 - x$. En vertu de l'hypothèse nous pouvons écrire la proportion suivante:

$$\frac{1}{x}=\frac{x}{1-x}, \tag{4.1}$$

d'où

$$x^2 = 1 - x. \tag{4.2}$$

La racine positive de (4.2) est $\frac{-1+\sqrt{5}}{2}$. Chaque rapport de la proportion (4.1) devient:

$$\frac{1}{x}=\frac{2}{-1+\sqrt{5}}=\frac{2(1+\sqrt{5})}{(-1+\sqrt{5})(1+\sqrt{5})}=\frac{1+\sqrt{5}}{2}=\alpha.$$

Cette division du segment AB par le point C_1 s'appelle *division en moyenne et extrême raison* (on dit aussi la *section dorée*).

Si nous considérons la racine négative de (4.2), le point C_2 qui lui correspond est alors à l'extérieur du segment AB. (On dit que C_2 partage AB extérieurement.) Il est facile de montrer que c'est encore la section dorée:

$$\frac{C_2B}{AB}=\frac{AB}{C_2A}=\alpha.$$



Fig. 2

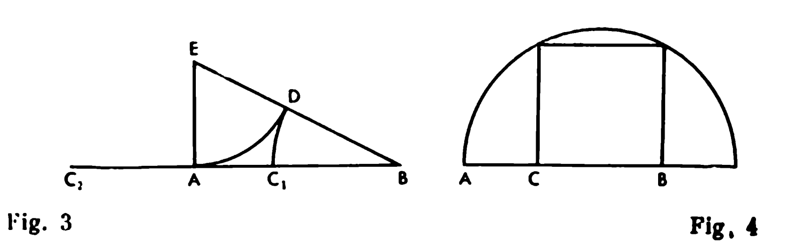


Fig. 3

Fig. 4

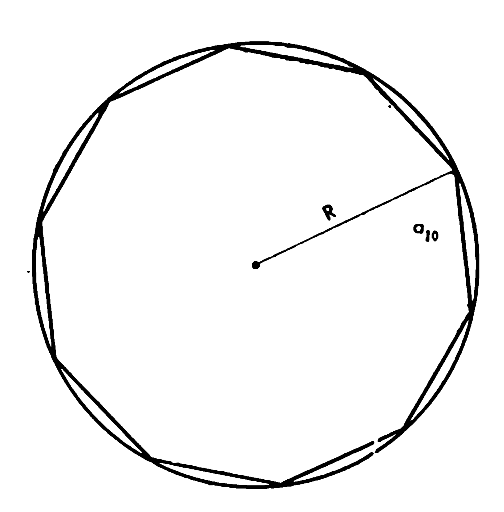


Fig. 5

2. On construit sans difficultés le point qui divise un segment en moyenne et extrême raison.

Soit $AB = 1$. Menons par A une perpendiculaire à la droite AB et fixons le point E tel que $AE = \frac{1}{2}$ (fig. 3). On a alors

$$EB = \sqrt{1 + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{5}}{2}.$$

Traçons un arc du cercle de centre E et de rayon EA. Cet arc coupe EB en D. Nous avons donc

$$BD = \frac{\sqrt{5}-1}{2}.$$

En menant à partir de B comme centre un arc du cercle de rayon BD nous déterminons sur AB un point qui est le point cherché C_1. On peut trouver le point C_2 qui partage extérieurement AB en utilisant l'égalité $AC_2 = BC_1$.

3. On use souvent en géométrie de la division en moyenne et extrême raison. Ainsi, pour un carré inscrit dans un demi-cercle la division par le point C du segment AB est la section dorée (v. fig. 4).

Dans un décagone régulier inscrit dans un cercle de rayon R (fig. 5), le côté a_{10} est égal à

$$2R \sin \frac{360°}{2 \cdot 10°},$$

c'est-à-dire $2R \sin 18°$.

Calculons sin 18°. En utilisant les formules trigonométriques connues on a :

$$\sin 36° = 2 \sin 18° \cos 18°,$$
$$\cos 36° = 1 - 2 \sin^2 18°,$$

de sorte que

$$\sin 72° = 4 \sin 18° \cos 18° (1 - 2 \sin^2 18°). \qquad (4.3)$$

Vu que $\sin 72° = \cos 18° \neq 0$, on déduit de (4.3) que

$$1 = 4 \sin 18° (1 - 2 \sin^2 18°),$$

et sin 18° est donc une racine de l'équiation

$$1 = 4x\,(1-2x^2)$$

ou de l'équation

$$8x^3 - 4x + 1 = 0.$$

Nous pouvons décomposer le premier membre de la dernière équation en un produit de facteurs. On obtient

$$(2x-1)\,(4x^2+2x-1) = 0,$$

$$x_1 = \frac{1}{2}, \quad x_2 = \frac{-1+\sqrt{5}}{4}, \quad x_3 = \frac{-1-\sqrt{5}}{4}.$$

d'où

Puisque sin 18° est un nombre positif différent de $\frac{1}{2}$, on a:

$$\sin 18° = \frac{\sqrt{5}-1}{4} = \frac{1}{2\alpha}.$$

Il faut remarquer que

$$\cos 36° = 1-2\sin^2 18° = 1-2\,\frac{1}{4\alpha^2} = 1-\frac{1}{2\alpha^2} =$$

$$= \frac{2\alpha^2-1}{2\alpha^2} = \frac{2+2\alpha-1}{2\alpha^2} = \frac{2\alpha+1}{2\alpha^2} = \frac{\alpha^3}{2\alpha^2} = \frac{\alpha}{2}.$$

Ainsi,

$$a_{10} = 2R\,\frac{\sqrt{5}-1}{4} = R\,\frac{\sqrt{5}-1}{2} = \frac{R}{\alpha}.$$

Ainsi, a_{10} est égal à la partie plus grande du rayon divisé en moyenne et extrême raison.

Lorsqu'on calcule a_{10}, on peut remplacer α par le rapport de deux termes consécutifs de la suite de Fibonacci (n° 20, § 1 ou n° 8, § 3) et prendre pour valeur approchée de a_{10} le nombre $\frac{8}{13}R$ ou même $\frac{5}{8}R$.

4. Considérons un polygone régulier de 5 côtés. Ses diagonales forment un pentagone étoilé régulier (fig. 6).

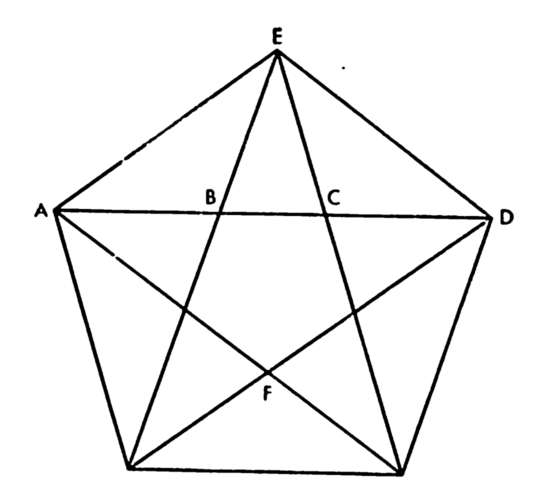


Fig. 6

L'angle AFD est égal à 108°, et l'angle ADF à 36°. On a d'après le théorème des sinus:

$$\frac{AD}{AF}=\frac{\sin 108^\circ}{\sin 36^\circ}=\frac{\sin 72^\circ}{\sin 36^\circ}=2\cos 36^\circ=2\frac{1+\sqrt{5}}{4}=\alpha.$$

Puisque $AF = AC$,

$$\frac{AD}{AF}=\frac{AD}{AC}=\alpha,$$

et le point C divise AD en moyenne et extrême raison.
Mais la définition de la section dorée nous fournit

$$\frac{AC}{CD}=\alpha.$$

Vu que $AB = CD$, il existe les égalités

$$\frac{AC}{AB}=\frac{AB}{BC}=\alpha.$$

Ainsi, dans la suite des segments BC, AB, AC, AD, chaque segment suivant est égal au segment précédent multiplié par α.

On propose au lecteur de vérifier que

$$\frac{AD}{AE}=\alpha.$$

5. Soit un rectangle de côtés a et b. Nous allons le partager en les plus grands carrés possible de façon indiquée sur la figure 7.

Les raisonnements du n° 5, § 2 montrent que cette division pour a et b entiers correspond à l'algorithme d'Euclide appliqué aux mêmes nombres a et b. Le nombre de carrés de mêmes dimensions est alors égal au quotient incomplet correspondant dans la décomposition de la fraction $\frac{a}{b}$ en fraction continue (n° 1, § 3).

Soit un rectangle dont les côtés forment un rapport égal au rapport de deux termes consécutifs de la suite de Fibonacci (fig. 8). Si nous le partageons en carrés de façon indiquée ci-dessus, d'après numéro 4 du § 3, tous les carrés sauf deux les plus petits sont différents.

Les côtés de tous ces carrés étant respectivement égaux à u_1, u_2, . . ., u_n, leur aire totale est donc

$$u_1^2+u_2^2+\ldots+u_n^2.$$

Nous retrouvons l'aire du rectangle donné, qui est le produit $u_n u_{n+1}$.

Ainsi,

$$u_1^2+u_2^2+\ldots+u_n^2=u_n u_{n+1}$$

quel que soit n. C'est la démonstration géométrique de la proposition du n° 4, § 1.

6. Soit maintenant un rectangle dont les côtés forment le rapport α. (Nous appellerons rectangles à section dorée de tels rectangles.)

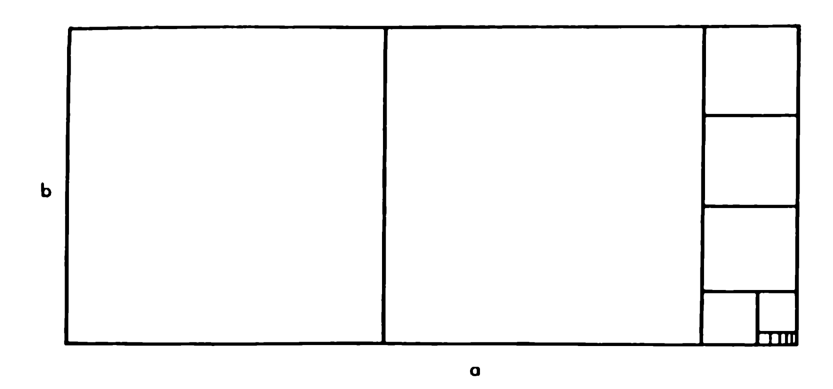


Fig. 7

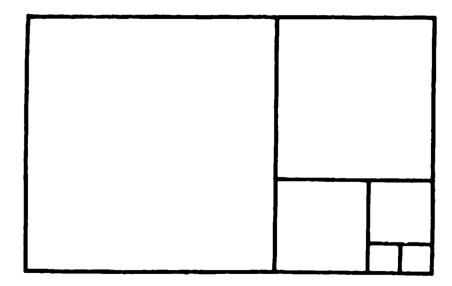


Fig. 8

Montrons que si on inscrit dans ce rectangle le plus grand carré possible, on obtient de nouveau un rectangle à section dorée (fig. 9).

En effet

$$\frac{AB}{AD} = \alpha;$$

par hypothèse $AD = AE = EF$, car $AEFD$ est un carré. D'où

$$\frac{EF}{EB} = \frac{AB - EB}{EB} = \alpha^2 - 1.$$

Or, $\alpha^2 - 1 = \alpha$, de sorte que

$$\frac{EF}{EB} = \alpha.$$

La figure 10 montre qu'un rectangle à section dorée peut être presque entièrement recouvert par les carrés *I*, *II*, *III*, . . . Chaque fois, après avoir inscrit un carré suivant, nous obtenons une figure qui est un rectangle à section dorée.

Nous proposons au lecteur de comparer ces raisonnements avec ceux des nos 4 et 8 du paragraphe précédent.

● REMARQUE. Si on inscrit dans un carré un rectangle à section dorée *I* et deux carrés *II* et *III* de façon indiquée sur la fig. 11, le rectangle qui reste est un rectangle à section dorée. Nous laissons au lecteur le soin de démontrer cette proposition.

7. La nature abonde en exemples d'objets homogènes dont la disposition est décrite par la suite de Fibonacci.

Toute disposition spiralée des parties des plantes présente en général deux familles de spirales. Les éléments de l'une tournent dans le sens des aiguilles d'une montre, et ceux de l'autre dans le sens opposé. Le nombre de spirales de la première famille et celui d'éléments de la deuxiè-

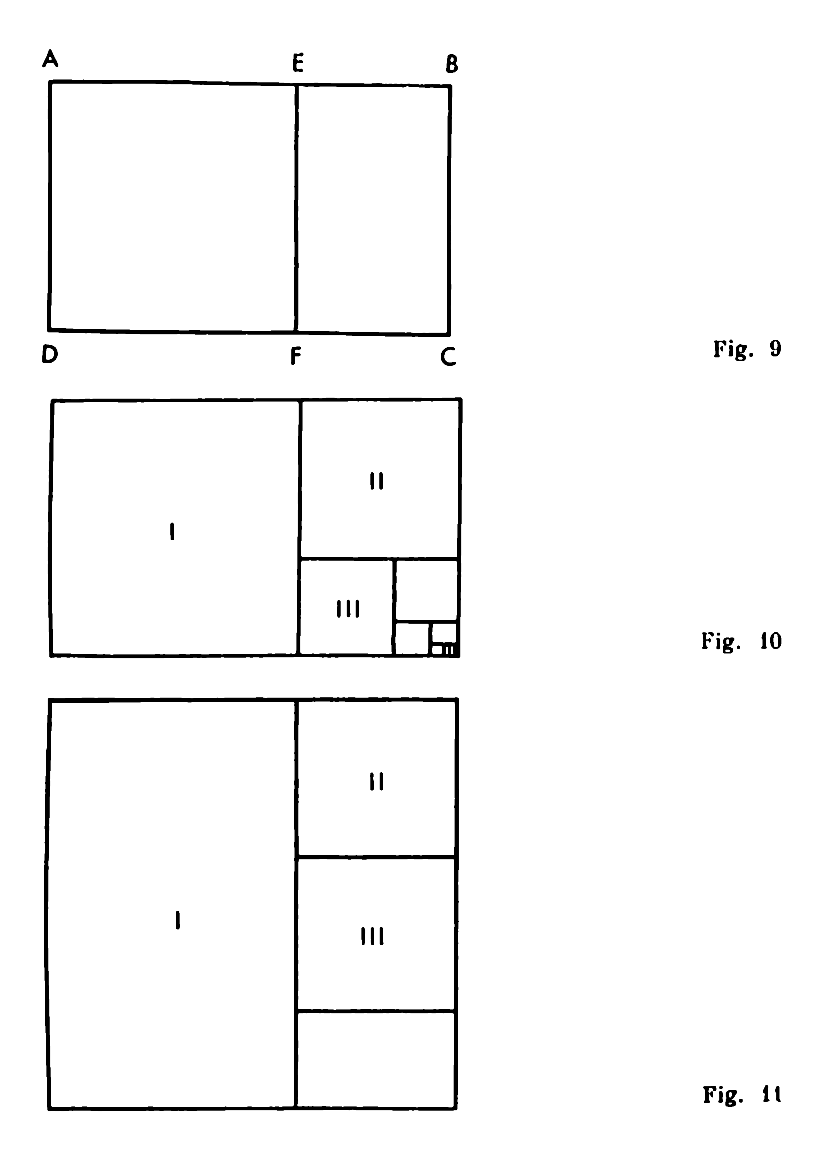


Fig. 9

Fig. 10

Fig. 11

me représentent souvent les termes consécutifs de la suite de Fibonacci.

Ainsi, il est facile de remarquer que les aiguilles d'une jeune branche de pin forment deux spirales s'élevant de droite à gauche. En même temps, elles forment trois spirales qui s'enroulent de gauche à droite.

Les écailles de nombreuses pommes de pin constituent l'ensemble de trois spirales s'enroulant doucement à leur axe. Elles forment d'autre part cinq spirales qui montent brusquement dans le sens opposé. Les grandes pommes de pin présentent parfois 5 et 8 spirales ou même 8 et 13. Un bon exemple de telles spirales nous donne un ananas (ordinairement elles y sont 8 et 13).

Les fleurs des capitules de nombreuses composées (la marguerite, la camomille) peuvent être disposées en spirale. Le nombre de spirales tournant dans les deux sens est respectivement 13 et 21 et, parfois, 21 et 34. Mais ce sont les graines du tournesol qui battent tous les records: les spirales qu'elles forment peuvent être 55 et 89 selon la direction.

8. Les rectangles à section dorée offrent de belles proportions et sont agréables à regarder. Il s'avère que l'usage d'objets ayant des formes pareilles est commode.

Certains philosophes idéalistes de l'Antiquité et du Moyen Age érigeaient les belles formes des rectangles à section dorée et d'autres figures admettant la division en moyenne et extrême raison en principe esthétique, voire philosophique. Ils se servaient de la section dorée et de certains autres rapports numériques non seulement pour décrire différents phénomènes naturels et sociaux, mais aussi pour les expliquer. Quant au nombre α et à ses fractions correspondantes, ils donnaient lieu à toutes sortes d'« opérations » mystiques. On conçoit que de pareilles « théories » n'ont rien d'une science.

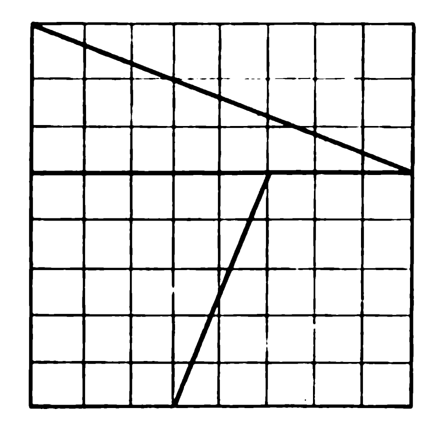


Fig. 12

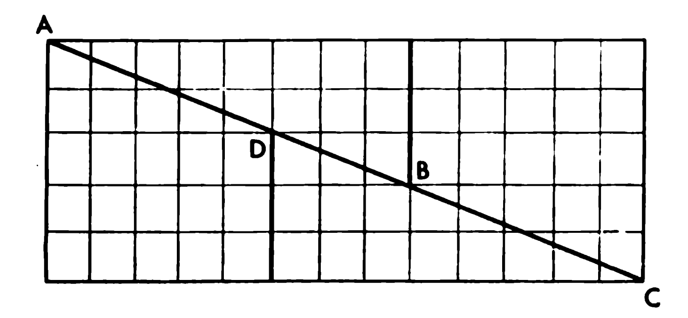


Fig. 13

9. Terminons notre exposé par un problème géométrique amusant. Nous allons démontrer que $64 = 65$. Considérons un carré dont le côté est égal à 8 et coupons-le en quatre parties de façon indiquée fig. 12. Formons avec un rectangle (fig. 13) dont les côtés sont respectivement égaux à 13 et 5 et dont l'aire est donc 65.

On explique facilement ce fait « mystérieux »: en réalité, les points A, B, C et D (fig. 13) ne sont pas alignés, mais coïncident avec les sommets d'un parallélogramme dont l'aire est justement égale à l'unité « de trop ».

De pareils raisonnements faux malgré une apparence de vérité s'appellent sophismes. La démonstration dans notre cas peut être encore plus convaincante si au lieu du carré de côté 8 on considère un carré tel que son côté soit égal à un certain terme u_{2n} de la suite de Fibonacci de numéro pair suffisamment grand. Divisons ce carré en parties (fig. 14) et construisons avec un rectangle (fig. 15). L'aire de l'interstice en forme d'un parallélogramme étendu le long de la diagonale est, d'après n° 9, § 1, égale à 1. On calcule aisément que la largeur maximale de l'interstice, c'est-à-dire la hauteur du parallélogramme, est égale à

$$\frac{1}{\sqrt{u_{2n}^2 + u_{2n-2}^2}}$$

Si l'on prend donc un carré dont le côté est égal à 21 cm et qu'on le transforme en un rectangle de côtés respectivement égaux à 34 et 13 cm, la largeur maximale de l'interstice est $\frac{1}{\sqrt{21^2+8^2}}$ cm, c'est-à-dire environ 0,4 mm, ce que l'œil ne discerne guère.

§ 5 SUITE DE FIBONACCI ET THÉORIE DE LA RECHERCHE

1. On ne sait que très bien qu'une auto consomme relativement beaucoup d'essence par kilomètre pour des vitesses

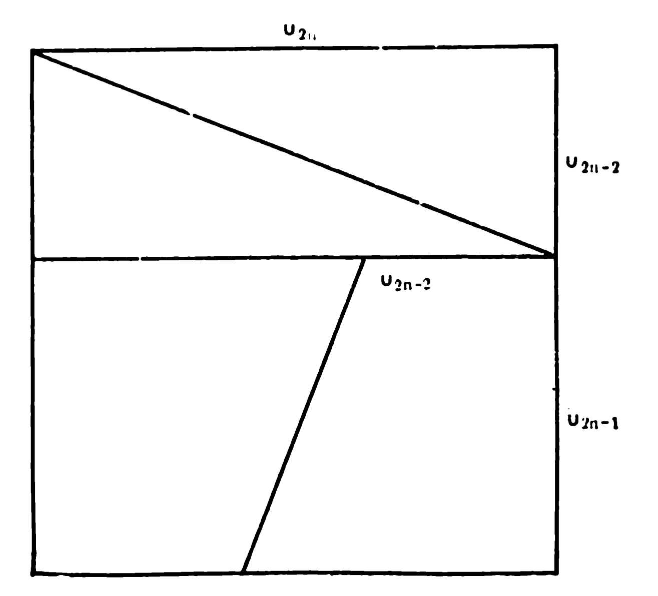


Fig. 14

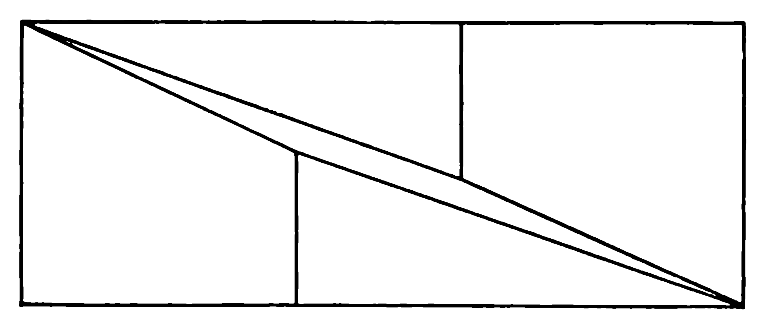


Fig. 15

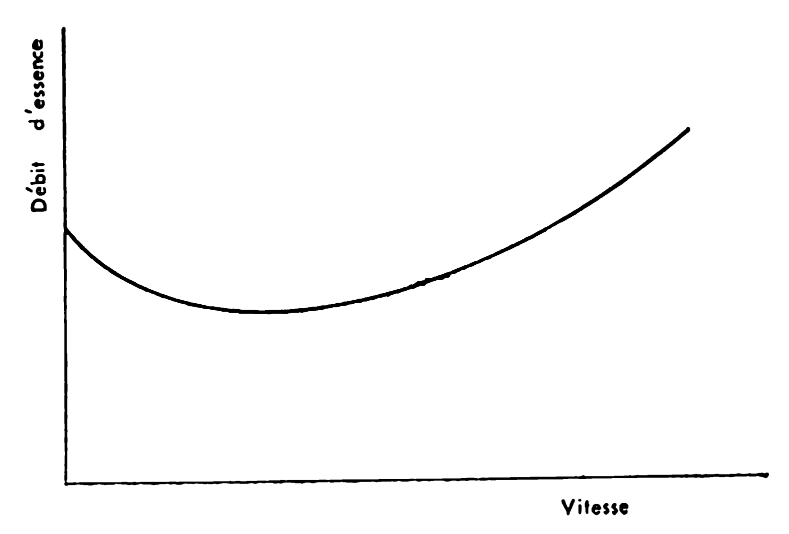


Fig. 16

assez petites. Il en est de même dans le cas des vitesses élevées. Ceci étant, une certaine vitesse intermédiaire est « optimale »: l'auto roulant à cette vitesse consomme le moins d'essence par kilomètre. Ainsi, nous sommes autorisé à supposer que le graphique approximatif de la relation entre la consommation d'essence par kilomètre et la vitesse de l'auto est de la forme donnée sur la figure 16. D'abord, le débit d'essence diminue jusqu'à la valeur minimale avec l'accroissement de la vitesse, puis, la vitesse augmentant toujours, il commence à croître sans cesse (un mathématicien parlerait de la croissance monotone).

Bien que l'allure de la courbe représentative de cette relation (une descente suivie d'une montée) soit pratiquement identique pour tous les automobiles, sa forme peut varier un peu, pour le même modèle de voitures, en fonction des particularités concrètes de l'auto, de

l'usure de ses mécanismes et dispositifs, etc. En particulier, la fonction que nous étudions peut présenter un minimum dans un intervalle assez vaste du graphique de la fig. 16.

Supposons que nous voulions partir en voyage en automobile et que la région à parcourir soit dépourvue de stations-services. Pour pouvoir couvrir la plus grande distance nous avons besoin de déterminer le plus exactement possible la vitesse qui correspondrait à la consommation d'essence minimale. Cette vitesse est appelée *vitesse la plus économique*.

Dans le cas d'une automobile il est naturel de déterminer cette vitesse en parcourant à des vitesses différentes plusieurs kilomètres d'une route dont les caractéristiques et la qualité préfigurent les conditions du voyage futur. On mesurera chaque kilomètre le débit d'essence. Ne vaut-il mieux, pour éviter cette corvée, d'essayer de répondre aux questions suivantes:

1° Combien d'expériences faut-il effectuer pour déterminer avec une précision donnée la vitesse la plus économique?

2° Pour quelles vitesses faut-il mesurer le débit d'essence? Deux autres questions s'y apparentent, à savoir comment faire pour que le nombre donné d'expériences fournisse la meilleure approximation? Quelle est cette meilleure approximation?

Ceci étant, nous sous-entendons par la vitesse la plus économique déterminée à un ε donné près la vitesse v telle que la valeur exacte de la vitesse la plus économique est comprise entre les nombres $v - \varepsilon$ et $v + \varepsilon$ (c'est-à-dire que l'erreur qu'on commet ne dépasse pas ε).

Pour fixer les idées supposons que la vitesse la plus économique de notre voiture se trouve entre v' et v''. Prenons pour v' une vitesse notoirement non supérieure à la vitesse la plus économique et pour v'' une vitesse qui ne lui est pas inférieure. (Par exemple, v' peut être la plus petite

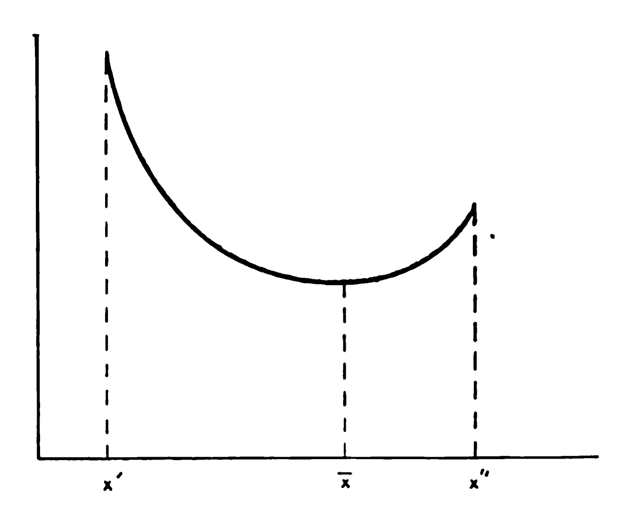


Fig. 17

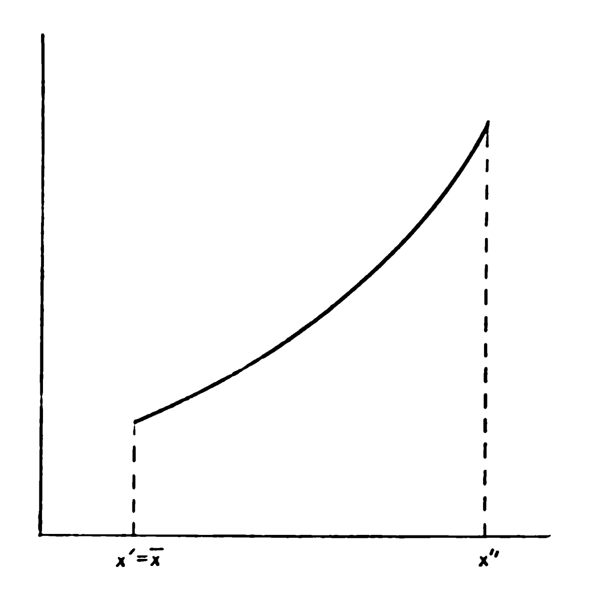


Fig. 18

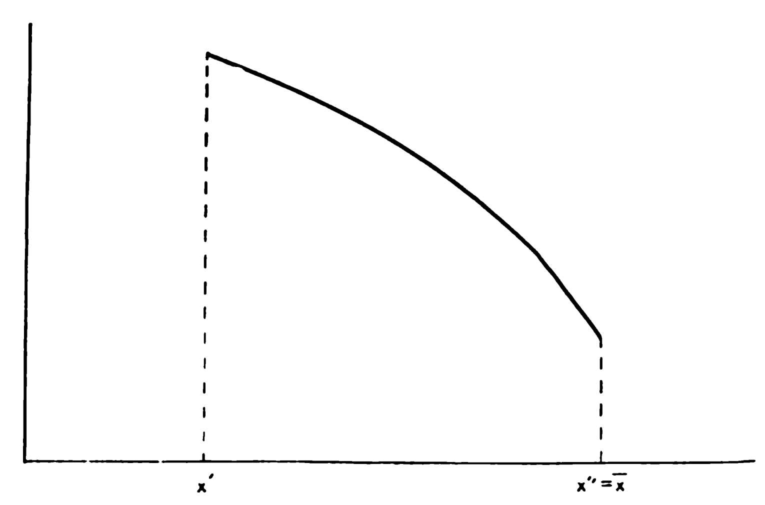


Fig. 19

vitesse pour laquelle le moteur fonctionne sans à-coups, et v'' est la vitesse maximale de notre voiture.)

2. Laissons de côté l'exemple concret que nous venons de considérer et étudions le problème mathématique suivant. Soit $f(x)$ une fonction dont on ne sait rien sinon qu'elle décroît de x' donné à un certain $\bar{x}$ et croît pour les valeurs de x comprises entre ce $\bar{x}$ et x'' donné (fig. 17). En particulier, nous admettons que le point inconnu $\bar{x}$ coïncide en réalité avec l'une des extrémités du segment, soit avec x' ou x''. Dans ce cas la fonction sera évidemment soit croissante (fig. 18) soit décroissante (fig. 19). Il va de soi que s'il en est ainsi, nous convenons de ne pas le savoir d'avance. Pour x égal à $\bar{x}$ la fonction f prend sa plus petite valeur $f(\bar{x})$ qui s'appelle valeur minimum ou simplement *minimum* de la fonction f. On dit alors que f présente un mini-

mum en $\bar{x}$ qui s'appelle encore *point de minimum* de la fonction.

Dans la suite nous ne considérerons que les fonctions qui ne peuvent pas être décroissantes après avoir être croissantes, et nous les appellerons *fonctions à un minimum.*

Nous nous proposons dans ce paragraphe d'analyser la possibilité de déterminer de façon exacte le point de minimum d'une fonction à un minimum. Par la fonction f nous sous-entendrons toujours une fonction à un minimum. Il est clair que *tout ce que nous dirons à propos des minimums des fonctions pourra être appliqué après des changements adéquats au cas de leurs maximums.*

3. Notre problème, tout comme beaucoup d'autres problèmes analogues, contient trois éléments constitutifs: les *buts* qu'on poursuit, les *possibilités* qu'on a pour les atteindre et les *conditions* dans lesquelles on utilise ces possibilités.

Dans notre cas le but consiste à déterminer avec une meilleure approximation le point de minimum, c'est-à-dire à diminuer l'erreur commise en indiquant ce point.

Sur le plan des possibilités nous pouvons déterminer exactement par tel ou tel moyen (calculer, mesurer ou, au pis aller, deviner) un certain nombre de valeurs de la fonction f en points quelconques et les comparer entre elles.

Enfin les conditions se déterminent par la grandeur du domaine de définition de la fonction f, c'est-à-dire par la longueur L du segment d'extrémités x' et x''.

Par conséquent, chaque problème de la recherche peut avoir trois aspects.

1° A quel point notre but est-il réalisable dans les conditions données compte tenu de nos possibilités? Cela signifie en termes de notre problème:

Supposons que n déterminations consécutives des valeurs de f soient possibles et qu'on n'impose aucune condition

au choix des points. En quels points faut-il déterminer les valeurs de la fonction pour que $\bar{x}$ soit trouvé avec la meilleure approximation, et quelle sera la précision?

2° Quelles doivent être nos possibilités pour pouvoir atteindre le but dans les conditions données?

Dans notre problème la question prend la forme suivante: soit à trouver une valeur approchée du point de minimum $\bar{x}$ de f à ε près, c'est-à-dire à indiquer x tel que $\bar{x}$ se trouve entre $x - \varepsilon$ et $x + \varepsilon$. Combien de valeurs de la fonction f est-il nécessaire de trouver à cette fin, et quel en est le procédé?

3° Dans quelles conditions les possibilités données sont-elles suffisantes pour atteindre le but?

Dans notre cas il s'agit de la recherche du plus grand intervalle de variation de la fonction f (c'est-à-dire de la plus grande valeur de la différence $x'' - x'$) pour lequel il existe un moyen de déterminer par n observations le point de minimum de f à ε près.

4. A proprement parler, nous aurons affaire à deux problèmes et non à un seul.

Premièrement, nous cherchons le point de minimum $\bar{x}$ *et* la valeur $f(\bar{x})$ que prend notre fonction f en ce point.

Deuxièmement, *seul* le point $\bar{x}$ nous intéresse.

On conçoit que le premier problème (nous l'appellerons problème A) est plus vaste que le deuxième (problème B). On s'attend donc naturellement que:

a) dans les conditions données et en tenant compte des possibilités, les buts du problème A seront plus difficiles à atteindre que ceux du problème B (étant donnés un nombre n et la longueur L, le problème B nous donne un ε plus petit que celui du problème A);

b) pour réaliser également les buts de deux problèmes dans les mêmes conditions, le problème A doit jouir de possibilités plus grandes (pour la même erreur ε et les mêmes

longueurs L des intervalles de variation de la fonction, n doit en général être plus grand dans le problème A);

c) la même réalisation des buts lorsque les possibilités sont les mêmes demande des conditions plus faciles dans le problème A (ε et n donnés dans le problème A ne sont compatibles qu'avec les valeurs de L inférieures à celles du problème B).

5. Pour formuler strictement les problèmes ci-dessus, une précision importante s'impose.

Admettons que nous nous intéressons aux possibilités de déterminer le point de minimum $\bar{x}$ dans le segment de longueur L (il est évident que nous pouvons considérer comme l'origine de ce segment le point 0 et comme l'extrémité le point L) à ε près. Supposons que nous devons résoudre le problème A, c'est-à-dire que $\bar{x}$ et $f(\bar{x})$ nous intéressent simultanément, et que le procédé de détermination de $\bar{x}$ est le suivant.

Fixons un point x quelconque entre 0 et L et déterminons les valeurs de la fonction f aux points $x - \varepsilon$, x et $x + \varepsilon$, c'est-à-dire calculons les valeurs $f(x - \varepsilon)$, $f(x)$, $f(x + \varepsilon)$ (fig. 20). En dépit du choix arbitraire de x, nous estimons que $x - \varepsilon \geqslant 0$ de sorte que la valeur de la fonction $f(x - \varepsilon)$ peut être calculée. De même on considère que $x + \varepsilon \leqslant L$.

Il peut arriver que

$$f(x-\varepsilon) > f(x) < f(x+\varepsilon).$$

Cela veut dire que la fonction f décroissante au point $x - \varepsilon$ commence à croître en passant vers $x + \varepsilon$. Mais un tel changement de sens de variation est lié à l'existence du minimum. Dans notre cas la fonction passe par cette valeur en un certain $\bar{x}$ compris entre $x - \varepsilon$ et $x + \varepsilon$.

C'est pourquoi x diffère de $\bar{x}$ par ε au plus et représente la valeur approchée de $\bar{x}$ que nous cherchons. Dans ce cas la détermination de $\bar{x}$ n'a lieu que par trois observations.

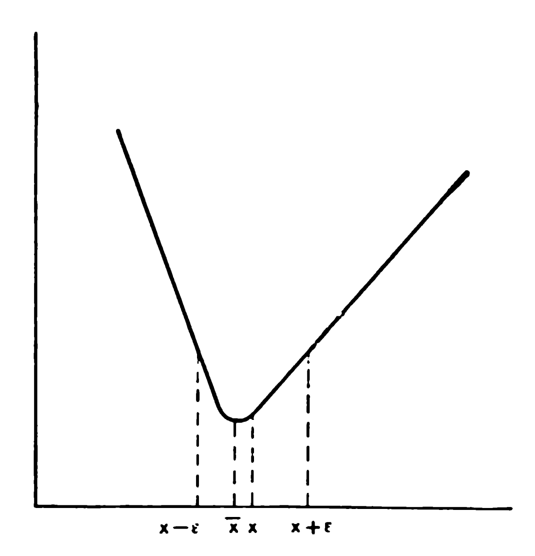


Fig. 20

Cela peut arriver, répétons-le. Mais rien ne nous garantit que cela *va* vraiment *arriver*. Il y a plus. Si la longueur L du segment est assez grande et ε assez petit, le phénomène paraîtra plutôt inattendu. Par contre, il est naturel qu'au voisinage des trois points fixes la fonction prend des valeurs assez grandes et qu'elle présente le minimum quelque part ailleurs. Trois observations sont donc suffisantes ou non selon le cas.

Or, nous avons besoin d'un procédé (d'une stratégie) qui nous permet *nécessairement* de déterminer $\bar{x}$ à ε près quel que soit le point x. De tels procédés existent. Calculons, par exemple, les valeurs successives de notre fonction

$$f(0),\ f(\varepsilon),\ f(2\varepsilon),\ \ldots \qquad (5.1)$$

jusqu'à ce qu'on aboutisse à $f(r\varepsilon)$ telle que $(r+1)\,\varepsilon$ soit supérieur à L (fig. 21). Il est clair que $k\varepsilon$ pour lequel la

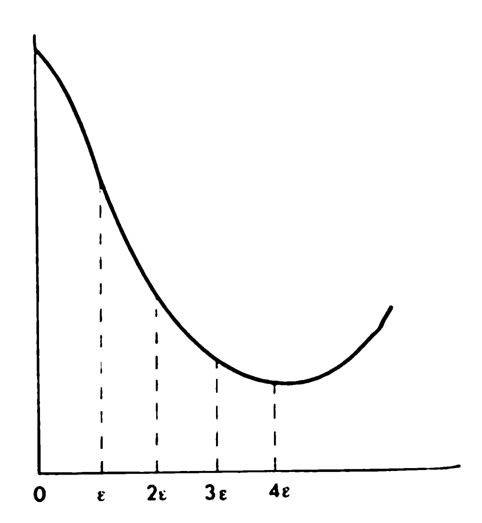


Fig. 21

valeur de la fonction dans la suite (5.1) est la plus petite est le nombre cherché.

En résolvant nos problèmes nous voulons élaborer plus qu'un simple procédé de calcul de $\bar{x}$ avec une précision donnée dans tous les cas, y compris les cas les moins favorables. Nous voulons mettre au point la stratégie *la plus économique*, c'est-à-dire la stratégie « *la meilleure dans les plus mauvaises conditions* ». Mais les plus mauvaises conditions sont celles dans lesquelles le nombre des valeurs calculées de la fonction f est maximal. D'une façon analogue la stratégie la plus économique est celle qui permet de réaliser le but avec le nombre minimal de valeurs calculées de la fonction.

C'est pourquoi la stratégie la meilleure dans les plus mauvaises conditions s'appelle souvent *stratégie de minimax*. Nous l'appellerons *stratégie optimale*.

Les opérations prévues par la stratégie optimale (qu'il s'agit de notre problème ou de n'importe quel autre problème analogue) consistent à rechercher de la façon la plus rationnelle le minimum de la fonction, qui « se cache » et qui « tâche d'être là où nous ne le cherchons point ». Tout ce qu'on vient de dire n'a rien à voir avec la mystique ni avec la superstition ; ce n'est que la caractéristique des meilleures opérations dans les plus mauvaises conditions.

6. Il est important de noter que tout problème de la recherche ne possède pas sa stratégie optimale. Il en est de même par exemple du problème B.

En effet soit $L = 2$ et $n = 2$. Quelle ε pouvons-nous garantir ?

Nous allons considérer les nombres 0 et 2 comme extrémités de notre segment. Soit α un nombre positif autant petit que l'on veut. Calculons les valeurs de la fonction f aux points $1 - \alpha$ et $1 + \alpha$. Si l'on a

$$f(1 - \alpha) \leqslant f(1 + \alpha),$$

le minimum cherché $\bar{x}$ doit être compris entre 0 et $1 + \alpha$, et si

$$f(1 - \alpha) \geqslant f(1 + \alpha),$$

$\bar{x}$ se trouve entre $1 - \alpha$ et 2.

Posons dans le premier cas

$$\bar{x} = \frac{1+\alpha}{2}$$

et

$$\bar{x} = \frac{(1-\alpha)+2}{2} = \frac{3-\alpha}{2}$$

dans le second.

Dans le plus mauvais cas $\bar{x}$ ainsi déterminé diffère de $\frac{1+\alpha}{2}$ du minimum vrai de la fonction f. En faisant approcher α de 0 nous diminuons l'erreur. Cependant α ne peut

pas être égal à 0. (Sinon les points $1 - \alpha$ et $1 + \alpha$ coïncident, et la comparaison de la valeur $f(1 - \alpha)$ avec la valeur $f(1 + \alpha)$ calculée au même point, qui lui est égale, ne nous donne aucune information.) C'est pourquoi l'erreur reste toujours supérieure à la moitié bien qu'elle puisse être aussi proche que l'on veut de ce nombre.

Chaque valeur positive de α détermine ici une certaine stratégie. Plus α est proche de 0, plus cette stratégie est meilleure. Puisque pour tout $\alpha > 0$ il existe un nombre positif qui lui est inférieur, pour toute stratégie on peut trouver une stratégie meilleure. Par conséquent, il n'y a pas de stratégie optimale pour le problème B.

Cependant, pour ce problème il existe des stratégies « quasi optimales » conduisant aux résultats qui ne se prêtent guère à l'amélioration. Plus exactement, quel que soit un nombre $\gamma > 0$ il existe une stratégie P_γ telle que toute autre stratégie diminue l'erreur due à P_γ de γ au plus.

7. La stratégie décrite par la suite (5.1) avec un ε assez petit par rapport à la longueur L du segment considéré n'est pas optimale. En l'utilisant nous serons obligés de faire tous les r calculs dans les plus mauvaises conditions.

Essayons de faire autrement. Calculons un terme sur deux dans la suite (5.1):

$$f(0),\ f(2\varepsilon),\ f(4\varepsilon),\ \ldots;$$

trouvons ensuite le plus petit terme de cette nouvelle suite (soit $f(2k\varepsilon)$ ce terme) et calculons deux valeurs de la fonction $f((2k - 1)\varepsilon)$ et $f((2k + 1)\varepsilon)$. L'une de trois valeurs de la variable $(2k - 1)\varepsilon$, $2k\varepsilon$ et $(2k + 1)\varepsilon$, pour laquelle la valeur de la fonction f est la plus petite de trois valeurs suivantes:

$$f((2k - 1)\varepsilon),\ f(2k\varepsilon),\ f((2k + 1)\varepsilon),$$

est évidemment $\bar{x}$ à ε près. Cette nouvelle stratégie permet d'atteindre le but dans les plus mauvaises conditions au bout

d'environ $\left(\frac{r}{2}+2\right)$ calculs. Pour r assez grands ce dernier nombre est beaucoup plus petit que celui prévu par la première stratégie.

Ainsi, la première stratégie n'est pas optimale. Pour des raisons analogues il en est en général de même de la deuxième.

Cependant il y a une différence essentielle entre ces deux stratégies: la deuxième ne prévoit que certains points en lesquels ou calcule les valeurs de la fonction, le choix des autres points étant fait par la comparaison des valeurs calculées. Nous savons intuitivement que le choix des meilleures opérations doit être lié à l'information sur les résultats des opérations antérieures. La deuxième stratégie est plus perfectionnée sous ce rapport. N'empêche qu'on peut en général la perfectionner au point d'aboutir à la stratégie optimale.

La recherche du minimum d'une fonction prévoit tout naturellement la comparaison de chaque valeur nouvellement obtenue avec telles ou telles valeurs trouvées antérieurement. Donc le choix du point en lequel on va prendre la valeur suivante (ou la décision de s'arrêter) dépend, d'une façon ou d'une autre, des points pour lesquels les valeurs de la fonction sont déjà calculées et des valeurs calculées de la fonction.

Evidemment, ce procédé de calcul successif des valeurs de la fonction f est bien déterminé par une certaine loi de correspondance qui, pour tout $k \geqslant 0$, fait correspondre aux ensembles arbitraires de points $x_1, x_2, \ldots, x_k$ et de valeurs numériques de f calculées en ces points un point quelconque x_{k+1} ou la décision de cesser les observations en choisissant un point quelconque pour $\bar{x}$. On appelle *fonction de décision* cette loi de correspondance.

Chaque stratégie détermine une certaine fonction de décision. Réciproquement toute fonction de décision détermine une certaine stratégie. En réalité, une fonction de décision est précisément une description nette et formalisée d'une stratégie. Par exemple, la fonction de décision qui détermine la première stratégie du numéro précé-

dont fait correspondre à chaque nombre $0 \leqslant k < r$ un point $(k+1)\,\varepsilon$ et au nombre r la fin du processus.

La notion de fonction de décision est l'une des plus importantes en mathématiques modernes. Malheureusement, la définition exacte de cette notion est assez volumineuse et ne peut pas être donnée ici.

8. Soit P une stratégie dont le but est de déterminer avec la meilleure approximation et par n observations le point $\bar{x}$ en lequel la fonction f atteint son minimum sur le segment de longueur L. Nous dirons que cette stratégie est *à n pas*.

Admettons que dans les conditions d'une certaine stratégie P à n pas nous réussissons à déterminer $\bar{x}$ sur le segment de longueur L à ε près. La précision dépend de P et aussi de n et de L. Ainsi, on peut la considérer comme fonction de P, n et L, et on la désigne par $\tau_P^A(n, L)$ pour le problème A et par $\tau_P^B(n, L)$ pour le problème B. Par le symbole $\tau_P(n, L)$ on sous-entend l'une ou l'autre des expressions $\tau_P^A(n, L)$ et $\tau_P^B(n, L)$ (on conçoit que cette expression est la même pour un même raisonnement).

La stratégie P_0 à n pas est optimale pour le problème A si $\tau_{P_0}^A(n, L)$ ne dépasse pas $\tau_P^A(n, L)$ pour toute autre stratégie P, c'est-à-dire que $\tau_{P_0}^A(n, L) \leqslant \tau_P^A(n, L)$. On peut l'écrire sous la forme:

$$\tau_{P_0}^A(n, L) = \min_P \tau_P^A(n, L). \tag{5.2}$$

Ainsi, le nombre $\tau_{P_0}^A(n, L)$ n'est plus la caractéristique de la stratégie, mais celle du problème même (à savoir la recherche par n pas du point de minimum de la fonction f sur le segment dont la longueur est égale à L). Il ne dépend pas d'une stratégie quelconque, mais seulement de n et L et peut être noté $\tau^A(n, L)$.

Dans les conditions du problème B tout est plus compliqué. Comme nous avons vu, il n'y a pas ici de stratégie optimale qui garantisse l'erreur la plus petite possible dans les plus mauvaises conditions. Cependant, il existe une

erreur dont on peut approcher autant que l'on veut si l'on choisit une stratégie convenable. Cette erreur qu'on appelle *erreur limite* ne dépend elle aussi que des conditions du problème. Il est logique donc de la noter $\tau^B(n, L)$. Toute autre stratégie amène à l'erreur plus grande

$$\tau^B(n, L) < \tau_P^B(n, L),$$

et nous ne pouvons écrire l'égalité analogue à (5.2).

En anticipant nous pouvons dire que tous les raisonnements de ce paragraphe (et ces raisonnements sont parfois compliqués) conduisent aux expressions explicites pour $\tau^A(n, L)$ et $\tau^B(n, L)$. Il s'avérera que ces expressions contiennent les termes de la suite de Fibonacci:

$$\tau^A(n, L) = \frac{L}{u_{n+2}}, \tag{5.3}$$

$$\tau^B(n, L) = \frac{L}{2u_{n+1}}. \tag{5.4}$$

Ainsi, si l'on refuse de chercher la valeur minimum d'une fonction, on améliore par là même $\frac{2u_{n+1}}{u_{n+2}}$ fois la détermination de son point de minimum. Pour n assez grands ce rapport d'après n° 13, § 1 est proche de $\frac{2}{\alpha} = 1{,}236$, ce qui correspond à une précision d'environ 23 % plus grande.

9. Il est clair que dans tout ce qui va suivre nous aurons besoin non pas des nombres L et ε pris isolément, mais de leur rapport qui s'appelle l'erreur relative sur la position de $\bar{x}$. Si ce rapport est donné, alors, pour un choix convenable de l'unité de mesure de x (c'est-à-dire l'unité de longueur) nous pouvons prendre arbitrairement L ou ε.

Une conclusion fort instructive s'impose.

Le changement d'échelle sur l'axe des x fait varier d'un même nombre de fois l'expression numérique de la longueur L du segment et l'erreur due à la détermination

du point cherché par toute stratégie P. Autrement dit, quel que soit λ positif, on doit avoir

$$\tau_P(n, \lambda L) = \lambda \tau_P(n, L). \tag{5.5}$$

De même, si, en décrivant une stratégie visant à déterminer le point de minimum, nous nous servons, pour indiquer la position des points du segment, non pas des mesures de longueur absolues mais des mesures relatives, la nature de la stratégie ne change pas: les stratégies optimales restent optimales, et les stratégies non optimales conservent cette propriété.

D'où il vient immédiatement que la dilatation (ou la compression) uniforme de n fois (où n est quelconque) de l'intervalle de variation de la fonction se borne à réaliser l'« homothétie » de la stratégie optimale sans compromettre son optimalité.

Donc, les erreurs $\tau_P(n, \lambda L)$ et $\tau_P(n, L)$ figurant dans l'égalité (5.5) ne sont pas dues qu'à la mise en pratique des stratégies différentes. Elles peuvent être considérées comme le résultat de l'application d'une même stratégie soumise aux différentes « homothéties ».

10. Après cette étude préliminaire assez longue passons à la recherche de la stratégie optimale pour le problème A et à la démonstration des formules (5.3) et (5.4).

● LEMME. *Quels que soient $n \geqslant 1$ et L, il existe une stratégie à n pas de la recherche du point $\bar{x}$ qui minimise la valeur de la fonction f (à un minimum) sur le segment de longueur L par n pas et qui possède les propriétés suivantes:*

1° *on considère à chaque pas un certain segment $x'x''$;*

2° *au premier pas on calcule la valeur de la fonction f en l'un des points: $\frac{u_n}{u_{n+2}} L$ et $\frac{u_{n+1}}{u_{n+2}} L$;*

3° *on effectue chaque pas suivant de numéro k (c'est-à-dire pour $1 < k \leqslant n$), en connaissant la valeur de f en l'un des*

points suivants:

$$x_1 = x' + \frac{u_n}{u_{n+2}}(x'' - x') \quad et \quad x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x'); \qquad (5.6)$$

4° *au* $k^{\text{ième}}$ *pas* $(1 < k \leqslant n)$ *on calcule la valeur de* f *en l'autre point* (5.6);

5° *au* $k^{\text{ième}}$ *pas* $(1 < k \leqslant n)$ *on compare les nombres* $f(x_1)$ *et* $f(x_2)$; *si* $f(x_1) \leqslant f(x_2)$, *on considère au* $(k+1)^{\text{ième}}$ *pas le segment* $x'x_2$, *et le segment* x_1x'' *si* $f(x_1) \geqslant f(x_2)$.

La démonstration se fait par récurrence sur n.

Si $n = 1$, le segment est évidemment déterminé par 0 et L; la valeur de la fonction est calculée au point $\frac{u_1}{u_3}L = \frac{L}{2}$; dans ce cas il n'y a plus de pas.

Admettons maintenant que l'existence d'une stratégie à n pas munie des propriétés du lemme est établie pour tout segment. Elaborons la stratégie à $(n+1)$ pas qui nous intéresse en vérifiant si les conditions du lemme sont satisfaites. Considérons à chaque pas un certain segment $x'x''$.

Prenons pour le premier pas le choix du point $x_1 = \frac{u_{n+1}}{u_{n+3}}L$ et pour le deuxième celui du point $x_2 = \frac{u_{n+2}}{u_{n+3}}L$ et la comparaison des valeurs $f(x_1)$ et $f(x_2)$. Le cas $f(x_1) \leqslant f(x_2)$ nous amène au segment déterminé par 0 et x_2 (x' est égal à 0 et x'' à x_2), le cas $f(x_1) > f(x_2)$ au segment déterminé par x_1 et L (x' est égal à x_1 et x'' à L). Dans les deux cas la longueur du segment considéré est égale à $\frac{u_{n+2}}{u_{n+3}}L$. Après ces deux pas nous nous trouvons, par rapport au segment considéré, dans les mêmes conditions qu'après avoir réalisé le premier pas du procédé à n pas.

Notamment, nous connaissons sur le segment de longueur $\frac{u_{n+2}}{u_{n+3}}L$ la valeur de la fonction f au point distant de

$\frac{u_{n+1}}{u_{n+3}} L$ de l'une de ses extrémités. C'est pourquoi nous pouvons « passer » à ce procédé à n pas et l'appliquer jusqu'à la fin. Selon l'hypothèse de récurrence, les conditions 3°, 4°, 5° sont vérifiées pour les derniers n pas. Par conséquent, il ne nous reste qu'à étudier les conditions initiales du deuxième pas et ce pas lui-même. Il est évident que le point $\frac{u_n}{u_{n+3}} L$ se met sous la forme de la première expression (5.6) pour $k = 2$ si on remplace n par $n + 1$; dans ces conditions, le rôle de la deuxième expression (5.6) incombe au point choisi $\frac{u_{n+2}}{u_{n+3}} L$.

Ainsi, le lemme est établi.

11. Nous appellerons *stratégie de Fibonacci à n pas* ou *stratégie* F_n tout court la stratégie à n pas dont l'existence a été prouvée par le lemme précédent.

● THÉORÈME. 1° *F_n est l'unique stratégie optimale à n pas.*

2° $\tau^A_{F_n}(n, L) = \frac{L}{u_{n+2}}$.

On fait la d é m o n s t r a t i o n par récurrence sur n.

Commençons par le cas $n = 1$ lorsqu'on choisit en qualité de $\bar{x}$ un certain point $\tilde{x}$ de l'intervalle de x' à x''. Il est clair que dans les conditions les plus défavorables l'erreur peut coïncider avec le plus grand des nombres $x'' - \tilde{x}$ et $\tilde{x} - x'$. Si ces nombres sont distincts, l'erreur maximale dépasse $\frac{L}{2}$, s'ils sont égaux, elle est $\frac{L}{2}$.

Ainsi, F_1 est la stratégie optimale à 1 pas, et

$$\tau^A_{F_1}(1, L) = \frac{L}{2} = \frac{L}{u_2}.$$

Pour $n = 2$ nous avons F_2 qui consiste à calculer et comparer les valeurs $f\left(\frac{1}{3} L\right)$ et $f\left(\frac{2}{3} L\right)$ et à choisir en

qualité de $\bar{x}$ les points

$$\frac{1}{3}L \quad \text{si} \quad f\left(\frac{1}{3}L\right) \leqslant f\left(\frac{2}{3}L\right),$$
$$\frac{2}{3}L \quad \text{si} \quad f\left(\frac{1}{3}L\right) > f\left(\frac{2}{3}L\right).$$

Il est facile de voir que l'erreur maximale due à la détermination de la valeur exacte de $\bar{x}$ est $\frac{L}{3} = \frac{L}{u_4}$:

$$\tau^A_{F_2}(2,\ L) = \frac{L}{u_4}.$$

N'importe quel autre choix du point conduit à des erreurs plus grandes.

La première partie de la démonstration est donc faite. Supposons maintenant que F_n possède la propriété imposée par le théorème et considérons les stratégies à $(n+1)$ pas.

Après avoir réalisé deux premières observations de la fonction f dans le cadre de F_{n+1} et comparé les deux valeurs trouvées, nous pouvons réduire le problème à l'application de F_n au segment de longueur $\frac{u_{n+2}}{u_{n+3}}L$, la valeur de la fonction f en un point de ce segment étant connue. L'erreur qui en résultera dans les conditions les plus défavorables est

$$\tau^A_{F_n}\left(n,\ \frac{u_{n+2}}{u_{n+3}}L\right) = \frac{u_{n+2}}{u_{n+3}}\tau^A_{F_n}(n,\ L) = \frac{u_{n+2}}{u_{n+3}}\frac{L}{u_{n+2}} = \frac{L}{u_{n+3}}.$$

Par conséquent,

$$\tau^A_{F_{n+1}}(n+1,\ L) = \frac{L}{u_{n+3}}.$$

Il nous faut encore démontrer que F_{n+1} est optimale.

Considérons les observations sur la fonction f en deux points quelconques $\tilde{x}_1$ et $\tilde{x}_2$ (pour fixer les idées on pose $\tilde{x}_1 < \tilde{x}_2$). La comparaison de $f(\tilde{x}_1)$ et $f(\tilde{x}_2)$ nous conduit à chercher le point $\bar{x}$ soit sur le segment $(0,\ \tilde{x}_2)$, soit sur le

segment $(\tilde{x}_1, L)$.

Si

$$\tilde{x}_1 < \frac{u_{n+1}}{u_{n+3}} L$$

et $f(\tilde{x}_1) > f(\tilde{x}_2)$, il nous faut chercher à l'aide d'un procédé à n pas le point de minimum de f sur le segment dont la longueur est $L - \tilde{x}_1$, c'est-à-dire plus grande que

$$L - \frac{u_{n+1}}{u_{n+3}} L = \frac{u_{n+3} - u_{n+1}}{u_{n+3}} L = \frac{u_{n+2}}{u_{n+3}} L.$$

Même si la position du point $\tilde{x}_2$ sur le segment est la plus favorable, d'après l'hypothèse de récurrence l'erreur sur la détermination sera supérieure à $\frac{L}{u_{n+3}}$.

Des raisonnements analogues montrent qu'une stratégie qui commence par le choix d'un point $\hat{x}_2$ tel que $\hat{x}_2 > \frac{u_{n+2}}{u_{n+3}} L$ peut, dans des conditions défavorables correspondantes, nous faire commettre une erreur plus grande sur la détermination de $\bar{x}$ que la stratégie F_{n+1}.

Soit maintenant

$$\tilde{x}_1 > \frac{u_{n+1}}{u_{n+3}} L.$$

Si x se trouve bien entre 0 et $\hat{x}_1$, il ne nous reste que $n-1$ observations à faire dans la recherche de sa position, et la longueur du segment est supérieure à $\frac{u_{n+1}}{u_{n+3}} L$. Donc, même la stratégie F_{n-1} (qui d'après la supposition est optimale dans ces conditions) nous fait faire une erreur plus grande que

$$\tau^A_{F_{n-1}}\left(n-1, \frac{u_{n+1}}{u_{n+3}} L\right) =$$

$$= \frac{u_{n+1}}{u_{n+3}} \tau^A_{F_{n-1}}(n-1, L) = \frac{u_{n+1}}{u_{n+3}} \frac{L}{u_{n+1}} = \frac{L}{u_{n+3}}.$$

On considère de façon analogue le cas

$$\tilde{x}_2 > \frac{u_{n+2}}{u_{n+3}} L.$$

F_{n+1} est donc la stratégie optimale, et le théorème est démontré.

Ainsi, le seul point de minimum de la fonction f peut être déterminé sur le segment de longueur L par n observations avec une erreur qui ne dépasse pas $\frac{L}{u_{n+2}}$.

Aussi n observations nous permettent-elles de déterminer le point de minimum de la fonction f avec une erreur inférieure ou égale à ε sur le segment dont la longueur ne dépasse pas εu_{n+2}.

Enfin, pour être sûr que le point de minimum de f est déterminé sur le segment de longueur L avec une erreur qui ne dépasse pas ε, il faut effectuer n observations telles que

$$u_{n+1} < \frac{L}{\varepsilon} \leqslant u_{n+2}.$$

Ainsi, nous avons trouvé les réponses à toutes les questions du nº 3.

12. On peut résoudre sans beaucoup de difficultés le problème B en utilisant la résolution du problème A.

Soit donné un segment de longueur L. Considérons sur ce segment les premiers $n-2$ pas de F_{n-1}. Nous aboutissons au segment de longueur $\frac{3L}{u_{n+1}}$ et d'extrémités x' et x''. On connaît la valeur de la fonction f en l'un des deux points

$$x_1 = x' + \frac{L}{u_{n+1}}, \quad x_2 = x' + \frac{2L}{u_{n+1}}.$$

Nous nous bornons au premier cas (l'étude de l'autre est analogue).

Ainsi, soit $f(x_1)$ la valeur connue. Choisissons un nombre γ quelconque inférieur en valeur absolue à $\frac{L}{u_{n+1}}$ et calcu-

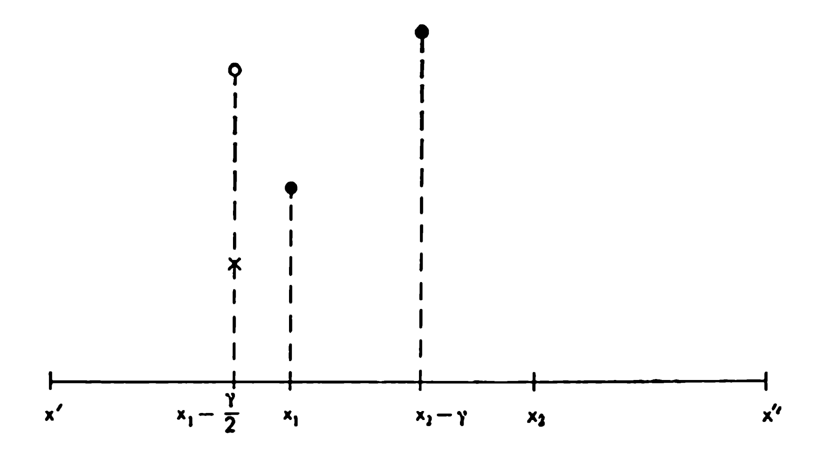


Fig. 22

lons $f(x_2 - \gamma)$ (c'est la $(n-1)^{\text{ième}}$ valeur numérique de f); comparons ensuite $f(x_1)$ et $f(x_2 - \gamma)$.

Si $f(x_1) \leqslant f(x_2 - \gamma)$ (fig. 22), il est évident que $\bar{x}$ se trouve entre x' et $x_2 - \gamma$. Calculons

$$f\left(\frac{x' + (x_2 - \gamma)}{2}\right) = f\left(x_1 - \frac{\gamma}{2}\right)$$

(c'est la dernière ($n^{\text{ième}}$) valeur trouvée de la fonction f). Si

$$f\left(x_1 - \frac{\gamma}{2}\right) \leqslant f(x_1)$$

(la croix sur la figure 22), alors $\bar{x}$ se trouve entre x' et x_1. Posons $\bar{x} = \frac{x' + x_1}{2}$. L'erreur sur la détermination de $\bar{x}$ ne dépasse pas la moitié de la longueur du segment de x'

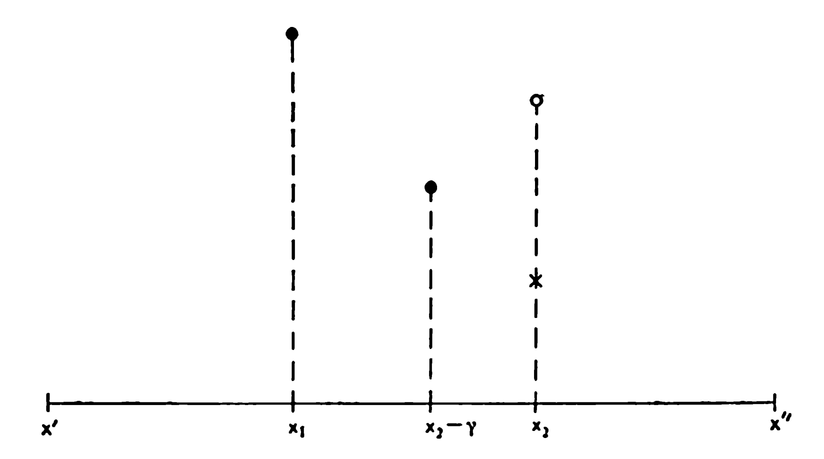


Fig. 23

à x_1, c'est-à-dire $\frac{L}{2u_{n+1}}$. Si $f\left(x_1-\frac{\gamma}{2}\right)>f(x_1)$ (le petit cercle blanc sur la fig. 22), $\bar{x}$ se trouve entre $x_1-\frac{\gamma}{2}$ et $x_2-\gamma$. En posant $\bar{x}=\frac{1}{2}\left(\left(x_1-\frac{\gamma}{2}\right)+(x_2-\gamma)\right)$, on commet une erreur qui ne dépasse pas

$$\frac{1}{2}\left((x_2-\gamma)-\left(x_1-\frac{\gamma}{2}\right)\right)=\frac{1}{2}\left(x_2-x_1-\frac{\gamma}{2}\right)=$$

$$=\frac{x_2-x_1}{2}-\frac{\gamma}{4}=\frac{L}{2u_{n+1}}-\frac{\gamma}{4}.$$

Soit maintenant $f(x_1)>f(x_2-\gamma)$ (fig. 23). Alors $\bar{x}$ se trouve entre x_1 et x''.

Calculons $f(x_2)$ (la dernière valeur numérique de f). Si

$$f(x_2-\gamma)\leqslant f(x_2)$$

(le petit cercle blanc sur la figure 23), $\bar{x}$ est compris entre x_1 et x_2;

en posant $\bar{x} = \frac{1}{2}(x_1 + x_2)$, on commet une erreur qui atteint à peine $\frac{1}{2}(x_2 - x_1) = \frac{L}{2u_{n+1}}$. Si enfin

$$f(x_2 - \gamma) > f(x_2)$$

(la croix sur la fig. 23), $\bar{x}$ se trouve entre $x_2 - \gamma$ et x''. En posant $\bar{x} = \frac{1}{2}(x'' + (x_2 - \gamma))$ on commet une erreur qui ne dépasse pas

$$\frac{1}{2}(x'' - (x_2 - \gamma)) = \frac{1}{2}\left(\frac{L}{u_{n+1}} + \gamma\right) = \frac{L}{2u_{n+1}} + \frac{\gamma}{2}.$$

Dans le plus mauvais cas, pour $\gamma > 0$, l'erreur peut atteindre la valeur $\frac{L}{2u_{n+1}} + \frac{\gamma}{2}$ et pour $\gamma < 0$ la valeur $\frac{L}{2u_{n+1}} - \frac{\gamma}{4}$. Mais puisque le choix du nombre γ est arbitraire, nous pouvons faire l'erreur aussi voisine que possible de $\frac{L}{2u_{n+1}}$.

Il nous reste à nous convaincre qu'il est impossible de diminuer l'erreur égale à $\frac{L}{2u_{n+1}}$.

En effet, en nous écartant à l'un quelconque des $(n - 2)$ premiers pas de la stratégie décrite, nous ne faisons d'après le théorème du nº 11 qu'augmenter la longueur du segment sur lequel la position du point de minimum se détermine par les mesures suivantes et par là même l'erreur maximale. Vérifions encore si les opérations effectuées aux deux derniers pas sont optimales.

Avant tout, l'écart aux opérations décrites peut signifier qu'on choisit définitivement pour $\bar{x}$ non pas le milieu du segment où il se trouve réellement mais un autre point quelconque. Il est clair que l'erreur possible s'avère alors égale à la plus grande partie du segment, c'est-à-dire qu'elle augmente. Donc il faut prendre justement le milieu du segment.

Ensuite, nous pouvons choisir pour la dernière détermina-

tion de f un point assez éloigné du point x_1 (ou respectivement de x_2). Mais cela implique une augmentation de l'erreur en proportion de la distance entre ces points.

Enfin, le fait de choisir pour l'avant-dernière détermination de f un point éloigné du point x_2 (respectivement de x_1) entraîne les mêmes conséquences.

Ainsi, aucun des écarts décrits ne peut diminuer l'erreur possible jusqu'à un nombre inférieur à $\frac{L}{2u_{n+1}}$. Cela prouve que le problème B est résolu.

Nous proposons au lecteur de donner, dans le cas du problème B, les réponses aux autres questions du n° 3.

13. Aux numéros précédents la description de la stratégie était complétée par les précisions portant sur la position du problème, par les formulations liées à la notion d'optimalité, par la justification du caractère optimal de la stratégie élaborée. Tous ces écarts à la description directe sont les éléments nécessaires de tout raisonnement mathématique qui vise non seulement à *indiquer* un procédé mais encore à *démontrer* que le procédé considéré est justement celui qui nous intéresse. D'autre part, la description des opérations comme telles importe seule dans de nombreux cas, tandis que la justification de ces opérations s'avère inessentielle. C'est le cas, par exemple, quand on se propose, une fois le problème résolu, de mettre en pratique la solution. Il importe peu alors que la solution soit ou non justifiée sur le plan mathématique; on a plutôt besoin d'un plan net, qui ne prête à aucune confusion, permettant de la réaliser.

Enoncé en conformité avec les raisonnements ci-dessus (c'est-à-dire qu'on poursuit des buts purement « pratiques »), le procédé de meilleure détermination du point $\bar{x}$ compris entre x' et x'' en lequel f présente le minimum dans les conditions du problème A fait penser au procédé d'identification d'une plante (oui, cette identification est bien une recherche!). Il est de la forme (sauf l'indication contraire,

on passe chaque fois au numéro qui suit):

1° Comparer 1 et n:

a) si $n = 1$, passer à 2°;

b) si $n > 1$, passer à 4°.

2° Calculer $\bar{x} = \frac{x' + x''}{2}$.

3° Calculer $f(\bar{x})$; le procédé s'arrête.

4° Calculer

$$x_1 = x' + \frac{u_n}{u_{n+2}}(x'' - x')$$

et

$$x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x').$$

5° Calculer $f(x_1)$ et $f(x_2)$.

6° Comparer 2 et n:

a) si $n = 2$, passer à 7°;

b) si $n > 2$, passer à 10°.

7° Comparer $f(x_1)$ et $f(x_2)$:

a) si $f(x_1) \leqslant f(x_2)$, passer à 8°;

b) si $f(x_1) > f(x_2)$, passer à 9°.

8° Poser $\bar{x} = x_1$ et terminer les opérations.

9° Poser $\bar{x} = x_2$ et terminer les opérations.

10° Comparer $f(x_1)$ et $f(x_2)$:

a) si $f(x_1) \leqslant f(x_2)$, passer à 11°;

b) si $f(x_1) > f(x_2)$, passer à 14°.

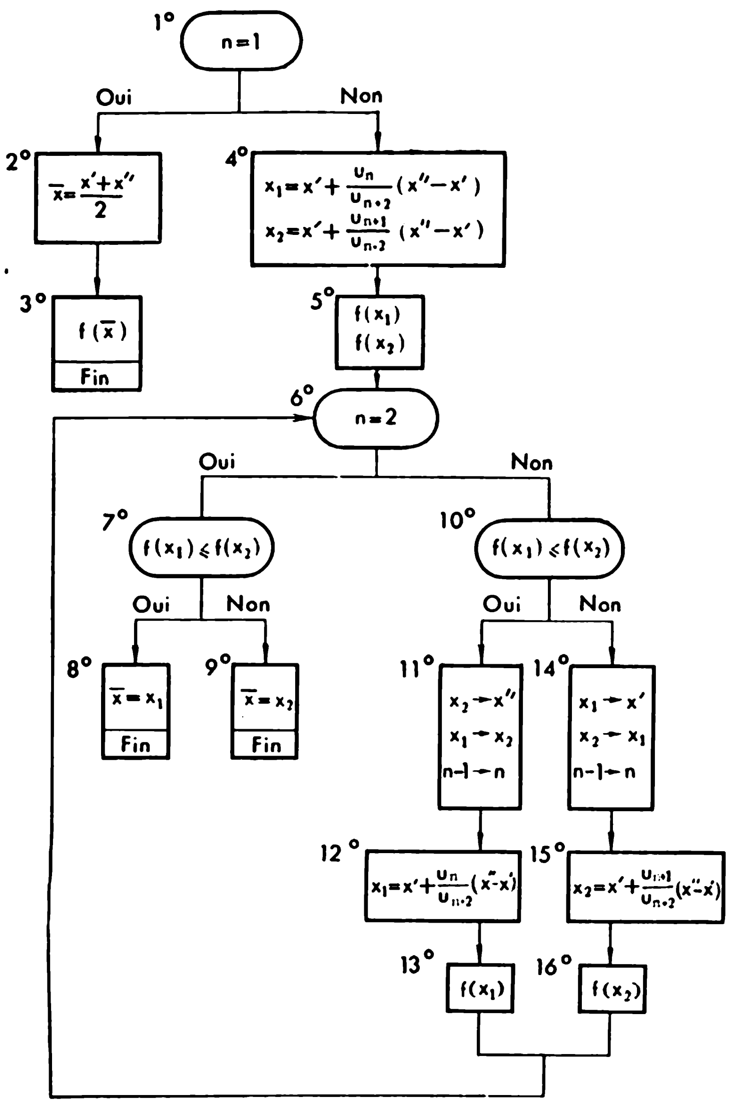
11° Désigner x_2 par x'', x_1 par x_2, $n - 1$ par n.

12° Calculer

$$x_1 = x' + \frac{u_n}{u_{n+2}}(x'' - x').$$

13° Calculer $f(x_1)$ et passer à 6°.

14° Désigner x_1 par x', x_2 par x_1, $n - 1$ par n.



1°
n=1
Oui
Non
2°
$\bar{x}=\frac{x'+x''}{2}$
4°
$x_1=x'+\frac{U_n}{U_{n+2}}(x''-x')$
$x_2=x'+\frac{U_{n+1}}{U_{n+2}}(x''-x')$
3°
$f(\bar{x})$
Fin
5°
$f(x_1)$
$f(x_2)$
6°
n=2
Oui
Non
7°
$f(x_1)\leqslant f(x_2)$
10°
$f(x_1)\leqslant f(x_2)$
Oui
Non
Oui
Non
8°
$\bar{x}=x_1$
Fin
9°
$\bar{x}=x_2$
Fin
11°
$x_2\rightarrow x''$
$x_1\rightarrow x_2$
$n-1\rightarrow n$
14°
$x_1\rightarrow x'$
$x_2\rightarrow x_1$
$n-1\rightarrow n$
12°
$x_1=x'+\frac{U_n}{U_{n+2}}(x''-x')$
15°
$x_2=x'+\frac{U_{n+1}}{U_{n+2}}(x''-x')$
13°
$f(x_1)$
16°
$f(x_2)$

Fig. 24

15° Calculer

$$x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x').$$

16° Calculer $f(x_2)$ et passer à 6°.

14. Bien que cette description soit nette et catégorique et qu'elle suppose dans le cas de chaque fonction f donnée la succession bien déterminée d'opérations sur le segment (x', x'') et le nombre n, elle est embrouillée et difficilement observable.

C'est pourquoi on va décrire notre procédé à l'aide d'un schéma (fig. 24) appelé *schéma bloc*. La mise au point d'un schéma bloc du procédé de calcul est la première étape de l'élaboration du programme des calculatrices électroniques numériques.

15. Pour conclure appliquons le procédé décrit aux n[os] 13 et 14 à la recherche, à l'aide de cinq calculs, du point de minimum $\bar{x}$ compris entre 1 et 2 de la fonction f telle que $f(x) = \frac{1}{x} + \sqrt{x}$.

Faisons au préalable une remarque importante.

Pour trouver le point de minimum (ou de maximum) d'une fonction représentée par une formule permettant de calculer ses valeurs, on a de préférence recours non pas aux méthodes de la théorie de la recherche, mais aux procédés plus adéquats se rapportant au calcul différentiel. Nous prévenons donc que l'exemple ci-dessous est purement illustratif. Le calcul différentiel permet de démontrer facilement que dans ce cas $\bar{x} = \sqrt[3]{4} = 1{,}5874011\ldots$ Or, nous obtenons une approximation infiniment plus grossière. Cependant, dans les cas où on ne sait rien d'avance de la fonction (sauf que sa croissance ne peut être suivie de la décroissance) ou si les expressions qui la déterminent sont très compliquées, on ne peut utiliser le calcul différentiel,

et la théorie de la recherche se trouve être un instrument efficace.

1° En comparant $n = 5$ et 1 on voit que $n \neq 1$; donc nous passons à 4°.

4° Calculons

$$x_1 = x' + \frac{u_n}{u_{n+2}}(x'' - x') = 1 + \frac{5}{13}(2-1) = 1{,}38461,$$

$$x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x') = 1 + \frac{8}{13}(2-1) = 1{,}61538.$$

5° Calculons

$$f(x_1) = \frac{1}{x_1} + \sqrt{x_1} = f(1{,}38461) = 0{,}72222 + 1{,}17670 = 1{,}89892,$$

$$f(x_2) = \frac{1}{x_2} + \sqrt{x_2} = f(1{,}61538) = 0{,}61905 + 1{,}27098 = 1{,}89003.$$

6° En comparant $n = 5$ et 2 nous obtenons $n \neq 2$; c'est pourquoi nous passons à 10°.

10° En comparant $f(x_1) = 1{,}89892$ et $f(x_2) = 1{,}89003$, on a $f(x_1) > f(x_2)$; donc nous passons à 14°.

14° Notons

$$x_1 \to x' = 1{,}38461,$$
$$x_2 \to x_1 = 1{,}61538,$$
$$n = 4.$$

15° Effectuons les calculs

$$x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x') = 1{,}38461 + \frac{5}{8}(2 - 1{,}38461) = 1{,}76927.$$

16° Calculons

$$f(x_2) = \frac{1}{x_2} + \sqrt{x_2} = f(1{,}76927) = 0{,}56522 + 1{,}33012 = 1{,}89534$$

et passons à 6°.

6° Comparons $n = 4$ et 2; puisque $n \neq 2$, passons à 10°.

10° Comparons $f(x_1) = 1{,}89003$ et $f(x_2) = 1{,}89534$; étant donné que $f(x_1) \leqslant f(x_2)$ passons à 11°.

11° Notons

$$x_2 \to x'' = 1{,}76923,$$
$$x_1 \to x_2 = 1{,}61538,$$
$$n = 3.$$

12° Effectuons les calculs

$$x_1 = x' + \frac{u_n}{u_{n+2}}(x'' - x') = 1{,}38461 + $$
$$+ \frac{2}{5}(1{,}76923 - 1{,}38461) = 1{,}53846.$$

13° Calculons

$$f(x_1) = \frac{1}{x_1} + \sqrt{x_1} = f(1{,}53846) = 0{,}65000 + 1{,}24035 = 1{,}89035$$

et passons à 6°.

6° Comparons $n = 3$ et 2; puisque $n \neq 2$, passons à 10°.

10° Comparons $f(x_1) = 1{,}89035$ et $f(x_2) = 1{,}89003$; puisque $f(x_1) > f(x_2)$, passons à 14°.

14° Notons

$$x_1 \to x' = 1{,}53846,$$
$$x_2 \to x_1 = 1{,}61538,$$
$$n = 2.$$

15° Calculons

$$x_2 = x' + \frac{u_{n+1}}{u_{n+2}}(x'' - x') = 1{,}53846 + $$
$$+ \frac{2}{3}(1{,}76923 - 1{,}53846) = 1{,}69231.$$

16° Effectuons les calculs

$$f(x_2) = \frac{1}{x_2} + \sqrt{x_2} = f(1{,}69231) = 0{,}59091 + 1{,}30089 = 1{,}89170$$

et passons à 6°.

6° La comparaison de n et 2 nous donne que $n = 2$; passons à 7°.

7° Comparons $f(x_1) = 1{,}89003$ et $f(x_2) = 1{,}89170$; $f(x_1) \leqslant f(x_2)$, donc nous passons à 8°.

8° Posons $\bar{x} = 1,61538$.

D'après le théorème du n° 11 cette valeur trouvée de $\bar{x}$ peut différer de la valeur vraie du point de minimum de $\frac{1}{u_{n+2}} = \frac{1}{u_7} = \frac{1}{13} = 0,077$ au plus. En réalité, cette erreur est plus petite ; elle est égale à 0,028. Remarquons que la valeur de la fonction f qu'on prend pour la plus petite, c'est-à-dire $f(x)$, est égale à 1,89003 et ne diffère que de 0,00015 de la plus petite valeur vraie qui est

$$f(\sqrt[3]{4}) = \frac{1}{\sqrt[3]{4}} + \sqrt[3]{2} = \frac{3}{2}\sqrt[3]{2} = 1,88988.$$

Cela montre que nous pouvions déterminer les valeurs de x avec une précision moins élevée que les valeurs de f.

Cette conclusion ne doit pas nous étonner. En effet, le calcul de x doit donner l'erreur limite qu'on commet dans nos conditions sur la position du point de minimum $\bar{x}$ $\left(\text{comme nous le savons, elle est égale à } \frac{1}{u_{n+2}}\right)$. Quant aux valeurs de f, elles doivent être calculées avec une précision permettant de comparer les couples de valeurs et de choisir dans chaque couple la plus petite et la plus grande valeur. Par conséquent, si la différence entre deux nombres quelconques $f(a)$ et $f(b)$ est sensible et qu'on le remarque même pour une détermination grossière de $f(a)$ et $f(b)$, nous pouvons les calculer avec une précision faible. Si, par contre, $f(a)$ et $f(b)$ sont proches l'une de l'autre, seul un calcul très précis permet de révéler le nombre le plus grand.

Puisqu'on ne sait pas d'avance (tant que les calculs ne sont pas finis) la différence entre les valeurs qu'on compare, on peut se tromper et les calculer avec une précision insuffisante, ce qui ne nous permettra pas de déterminer la plus grande valeur. Dans ce cas, des calculs plus précis s'imposent.

TABLE DES MATIÈRES